PROSUM

KLE

Keyboard Video Mouse IP Extender

User Manual
Revision 1.6
7/20/2007

Copyright and trademarks

Copyright © 2007 PROSUM. All rights reserved

All trademarks in this manual are the properties of their respective trademark owners.

About this manual

This User Guide is the complete reference to the KLE, its functional features and usage. The Complete User Guide could be found only on the KLE Support CD-ROM disc.

KLE documentation List

Quick Installation Guide	Print-out / KLE support CD-ROM disc
User Guide	KLE Support CD-ROM disc
How to generate your own set of Certificates	KLE Support CD-ROM disc

FCC Statement

This equipment has been tested and found to comply with the regulations for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this User Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case, the user will be required to correct the interference at his/her own expense.

CE Statement

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FC CE

Table of Contents

CHAPTER 1 ADVANTAGES AND FEATURES 1

1.1 ADVANTAGES 1
1.2 PRIMARY FEATURES 3
1.2.1 General features 3
1.2.2 TCP/IP remote connection 3
1.2.3 Thin-client Viewer Program 3
1.2.4 Hi-Speed PPP Connection 3
1.2.5 Video server 3
1.2.6 Power ON-OFF Control Support 3
1.2.7 Security 3
1.2.8 Alarms and Notifications 4
1.2.9 User Management 4
1.2.10 Global Time Zone Support 4
1.3 SYSTEM ARCHITECTURE 5
1.3.1 LAN/WAN Configurations 5
1.3.2 Power Control Configuration 6
1.3.3 PPP connections 6
1.4 KLE EXTERNAL VIEWS 8
1.4.1 KLE Front Panel 8
1.4.2 KLE Rear Panel 8
1.4.3 KLE Power Socket 9

CHAPTER 2 INSTALLING KLE 10

2.1 PHYSICAL CONNECTIONS 10
2.2 CONFIGURE YOUR SERVERS FOR CONNECTIONS TO KLE 12
2.2.1 Turn off mouse acceleration & "Snap to" option 12
2.3 MORE TIPS FOR SERVER DESKTOP CONFIGURATION 14
2.3.1 Configure the display resolution on your server 14
2.3.2 Disable special transition effects on the screen outputs of your connected servers 14
2.3.3 Choose plain and solid server desktop backgrounds for your connected servers. 15
2.4 KLE NETWORK SETTINGS 16
2.4.1 IP Settings 16
2.4.2 Port Base 17
2.5 CONFIGURING YOUR FIREWALL AND ROUTER FOR ACCESSING KLE ACROSS THE INTERNET 18
2.6 SECURITY SETTINGS 19
2.6.1 Select a User Password Policy 19
2.6.2 Select a Security Level for Viewer Connection 19
2.6.3 Installing Certificates and Key on KLE for Security level 3 20
2.6.4 Remote Clients 22

CHAPTER 3 VIEWER CONNECTION 23

3.1 INSTALLING THE VIEWERS ON THE CLIENT COMPUTER 23
3.1.1 Win32 Viewer 23
3.1.2 Java Viewer 23
3.2 INSTALLING CERTIFICATES ON THE CLIENT COMPUTER 24
3.2.1 Win32 Viewer 24
3.2.2 Java-based Viewer 24
3.3 STARTING THE VIEWER CONNECTION 25
3.3.1 Specifying the Viewer Connection Options 25
3.3.2 User Name and Password 25
3.4 SOME TIPS ABOUT VIEWER CONNECTIONS 27
3.4.1 Typing the KLE IP Address 27
3.4.2 Connection Performance Tuning 27

3.4.3 Local and Remote Mouse Cursor Synchronization *27*
3.5 SAVING THE CONNECTION OPTIONS 28
3.6 ADJUSTING THE VIEWER WINDOW SIZE 29
3.6.1 Changing the Viewer Size to Full Screen (Win32 Viewer only) *29*
3.6.2 Scaling the Viewer Window *30*
3.6.3 Centralizing the control of your remote servers *30*
3.7 VIEWER TITLE BAR INFORMATION 31
3.8 THE SELECT COMPUTER BOX 32
3.8.1 Win32 Viewer *32*
3.8.2 Java Viewer *32*
3.9 VIEWER QUICK MENU 33
3.9.1 Opening the Viewer Menu *33*
3.9.2 Menu Items *34*
3.10 VIDEO DISPLAY PROBLEM TROUBLESHOOTING 36

CHAPTER 4 KLE UNIT MANAGEMENT 39

4.1 WEB-BASED MANAGEMENT INTERFACE 39
4.2 USER PRIVILEGES – SUPERADMIN, ADMIN, USER 40
4.3 DOWNLOAD/VIEWERS – DOWNLOAD PROGRAMS FOR VIEWERS 41
4.4 MAIN/DATE & TIME – DATE, TIME, GLOBAL TIME ZONE SUPPORT AND NTP SERVER SYNCHRONIZATION 42
4.5 MAIN/SECURITY – CERTIFICATES, VIEWER ENCRYPTION AND PASSWORD POLICIES 43
4.5.1 Certificates and Keys *43*
4.5.2 Security Level of Viewer Connections *43*
4.5.3 User Password *44*
4.6 MAIN/TCP/IP SETTINGS – PORT AND IP SETTINGS 45
4.7 MAIN/WAN PPP 46
4.7.1 PPP Modes *46*
4.7.2 PPP Server Settings *47*
4.7.3 PPP Client Settings *48*
4.8 KVM SERVER/LOG 49
4.9 KVM SERVER/MAIN SETTING 50
4.9.1 Video Quality *50*
4.9.2 Attached KVM *51*
4.9.3 Scanning *51*
4.10 KVM SERVER/VIEWER CONNECTION – VIDEO SERVER NAME AND KEYBOARD TYPE SETTINGS 52
4.11 KVM SERVER/COMPUTERS – PORT AND IP SETTINGS 54
4.12 KVM SERVER/POWER CONTROL – ENABLE THE POWER CONTROL 56
4.13 KVM SERVER/KVM SWITCH DATABASE – KEEPING AND ADDING YOUR KVM DATABASE 59
4.14 KVM SERVER/VIDEO MODE DATABASE –MODIFYING THE VIDEO DISPLAY DATABASE 62
4.15 USERS/LOCAL DATABASE - MANAGING THE USER ACCOUNTS 64
4.16 USERS/REMOTE SERVERS – TUNING IN WITH THE REMOTE AUTHENTICATION SERVERS 66
4.16.1 Directory Server *66*
4.16.2 RADIUS Server *67*
4.17 USERS/RADIUS ACCOUNTING 68
4.18 USERS/CURRENT STATUS – SHOWING THE CURRENTLY CONNECTED USERS 69
4.19 ALARMS/EMAILS – SENDING EMAIL NOTIFICATIONS FOR CRITICAL SERVER EVENTS 70
4.20 ALARMS/SNMP – SENDING SNMP MESSAGES FOR CRITICAL SERVER EVENTS 71
4.21 ALARMS/SELECTIONS – SELECT THE ALARM-TRIGGERING EVENTS 72
4.22 MAINTENANCE/SOFTWARE VERSION – FLASH IMAGE INFORMATION 74
4.23 MAINTENANCE/SOFTWARE UPGRADE –UPGRADING THE SOFTWARE VIA WEB 75
4.24 MAINTENANCE/CONFIGURATION SAVE AND RESTORE 76
4.25 MAINTENANCE/REBOOT – CONFIGURATION BACKUP AND UPLOAD 77
4.26 APPLY SETTINGS/RESTART SERVERS – VALIDATE NEW SETTINGS & RESTART VIDEO SERVERS 78

Chapter 1
Advantages and Features

1.1 Advantages

KLE stands for **K**VM **L**ink **E**xtender. Though lightweight in size and compact in form factor, KLE is nevertheless heavy in its functional versatility, rock-solid robustness, and formidable security. It supports full 1024-bit PKI authentication, 256-bit SSL data encryption, LDAP, RADIUS as well Active Directory authentication and RADIUS accounting.

Dominant yet cost-effective solution for remote server management
With the ubiquity of the DSL/Cable technology and the bandwidth availability therewith, the IP-based KVM technology has emerged as a dominant player in the new landscape of remote servers management. Today, the IP-based KVM Extender has been regarded as a better and more cost-effective solution to address the critical issue of remote servers management, which could only be partially tackled in the past by expensive yet redundant software solutions or Enterprise Management System. KLE is a robust and versatile solution to address the needs of modern remote server management scenarios.

Total server control from BIOS level up anytime anywhere
KLE gives users total control from reboot stage such as the BIOS-level CMOS setting up to the GUI applications and daily maintenance routines such as power cycling (power control unit required). All these could be nicely done on your admin desk using an ordinary web-browser management interface and a thin-client software viewer. All you need for accessing your computer is to login to KLE and download the viewer program. Then you get yourself connected to a whole bunch of servers in seconds. A truly anytime anywhere access for the server administrator!

Versatile backup connection featuring a PPP Server or PPP Client
To provide the necessary redundancy of a second backup system while your network might no longer works in critical situation, KLE also allows an easy and convenient PPP connection over the dial-in modem phone line. It could serve as a PPP server to accept a peer computer to make PPP connection request over either a direct cable connection or a dial-in modem phone line. On the other hand, KLE could also serve as a PPP client to dial-in to your ISP or enterprise PPP server to connect to internet, making a truly anytime access for remote client anywhere on the Internet. Thus, the PPP server/client features in KLE allow users a second backup system, which offers a direct cable/modem dial-in access to your connected servers via PSTN while your network is down.

KLE – the KVM Link Extender

Edge of critical advantage over other remote server management solution
The advantages of using KLE, as compared to the conventional software remote control solution is that: The hardware-based remote control solution such as KLE is able to access the server regardless of the server states while software remote control solution is non-functional while the server is still in the POST or reboot stage or in a “blue screen of death”. KLE also offers power on/off alternatives if used with a remote power control unit.

Rock-solid stability and ultra-security yet with flexibility and convenience to use
KLE distinguishes itself among its peer products not only in its rock-solid stability in durable performance, but also in its industry-standard security features such as full 1024-bit PKI Authentication and 256-bit SSL data encryption. Together with 3 levels of viewer connection security levels in combination with 3 types of password policies and three categories of user privileges, all these make KLE a ultra-powerful IP Extender machine with ultra-flexibility for a customized balance between data safety and user convenience. On the other hand, the robustness and the ease of maintenance of the embedded systems involve zero costs for the unit management and maintenance.

Upgrade and Configuration Backup is just a breeze
KLE is fully Web-enabled to allow software upgrade and configuration upload/backup over the web management Interface. All you need to do is to upload the files to KLE over Web interface and voila it's freshly restarted and begins working with those latest update functionalities and features-all within minutes and can be performed across oceans-by a remote SUPERADMIN!

Advantages Galore
With KLE, the server administrator can access enterprise server room or data center on his own seat without toils and troubles of going anywhere from across the street, to oversea. Organizations can enjoy a uniquely centralized and very cost-effective control over its dispersed servers in different branch offices, even around the world, thus saving money for outsourcing costs.

1.2 Primary features

1.2.1 General features

- Full-featured IP-based Remote Control Solution for server management
- Provides remote control for several servers when connected to a conventional KVM Switch
- Simultaneous access from multiple users
- No user limitation
- Facilitate centralized control
- Total control over the remote server from BIOS level up to GUI applications
- Remote Power On/Off support
- Total transparency of control
- Ultra-security using full 1024-bit PKI Authentication / 256-bit SSL encryption
- Work with LDAP / RADIUS / Active Directory Servers
- Ethernet 10/100 and serial PPP connections

1.2.2 TCP/IP remote connection

- Web management Interface for all settings and upgrade/backup features
- Support Telnet session and FTP service (disabled by default for more security)

1.2.3 Thin-client Viewer Program

- Win-32 viewer and Java viewer for cross-platform compatibility
- Connection options configurable for optimized performance
- Shared, Non-Shared and View Only sessions
- Easy download and installation
- Multiple viewer instances can be run on a same client computer
- Automatic video optimization

1.2.4 Hi-Speed PPP Connection

- PPP Connection support over serial RS-232 interface up to 1 Mbps
- PPP server enabling for PPP connection across a pair of modems for secure or backup direct access
- PPP client enabling for PPP connection to the internet with a modem

1.2.5 Video server

- Support up to 1600 x 1200 @ 60 Hz resolution
- 8/16-bit color
- 3 Video Quality settings
- 4 Video Compression schemes
- 8-bit color reduction
- Configurable database to set up new or unknown VGA modes
- Virtually compatible to any KVM Switch through simple configuration

1.2.6 Power ON-OFF Control Support

- Remote power ON-OFF control over serial interface
- Serial commands configurable to fit all serial power control devices
- Power ON-OFF privilege only for the SUPERADMIN users

1.2.7 Security

- 1024-bit Public key Authentication using certificates generated by an external CA
- 256-bit SSL Encryption for keyboard, mouse and video signal transmissions
- Remote authentication support for LDAP or RADIUS servers
- RADIUS accounting support
- 3 SSL security levels:
    - No authentication – No encryption
    - Server Authentication – SSL encryption
    - Server & Client authentication – SSL encryption

- 3 password policies:
    - No Password
    - One global password for all users
    - One different password for each user
- Linux operating system offers robust virus resistance

1.2.8 Alarms and Notifications

- Alert e-mail notification and SNMP trap messages for critical server events such as No Video, Blue Screen and NumLock Test Failure
-

1.2.9 User Management

- User login either by querying the local user database or by connection to remote LDAP or RADIUS server
- 3 user privileges:
    - SUPERADMIN – to access complete set of management features and user features, including Power ON-OFF remote servers
    - ADMIN – partial set of management and all user features
    - USER – only user features

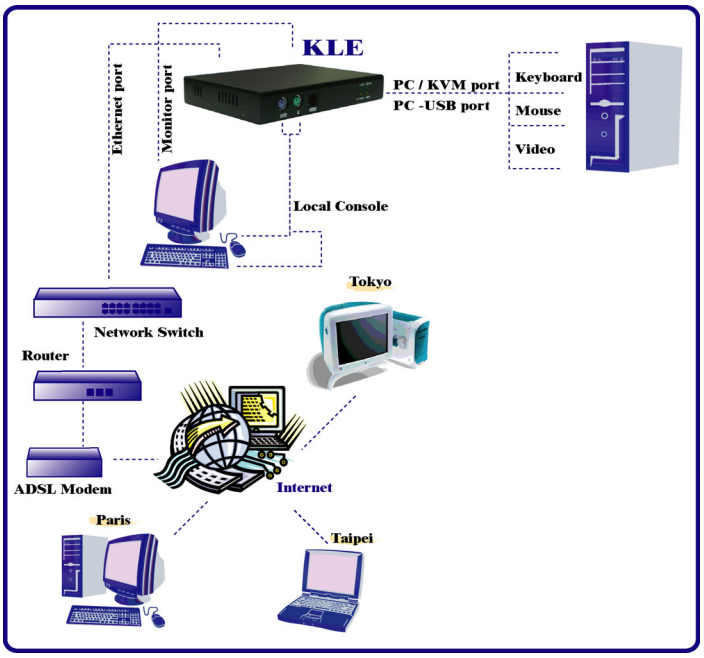
1.2.10 Global Time Zone Support

- Time support for all continents and major cities
- Time synchronization by connection to any NTP time servers
- Automatic Daylight Saving management

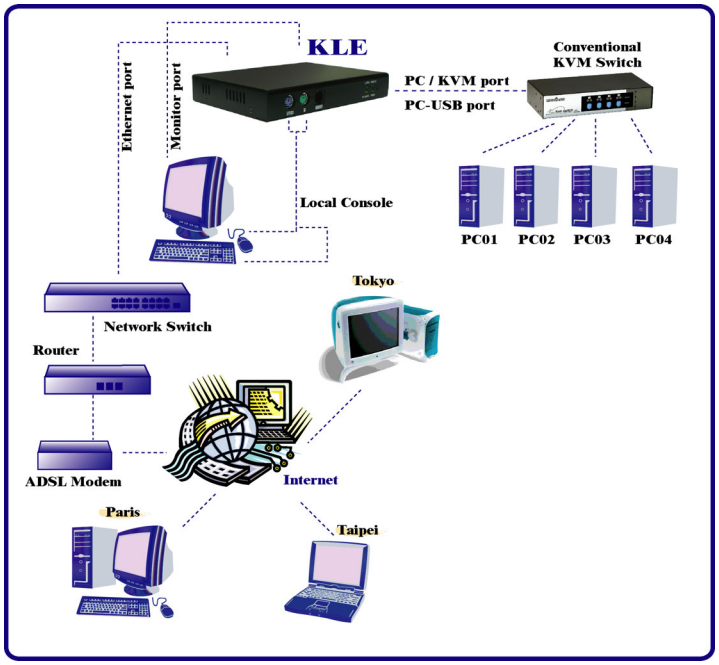
1.3 System Architecture

KLE is based on an embedded Linux platform for computing power and rugged stability. KLE employs a High speed Processor to ensure excellent video quality and fast keyboard / mouse response across the Internet, even when bandwidth availability is limited.

1.3.1 LAN/WAN Configurations

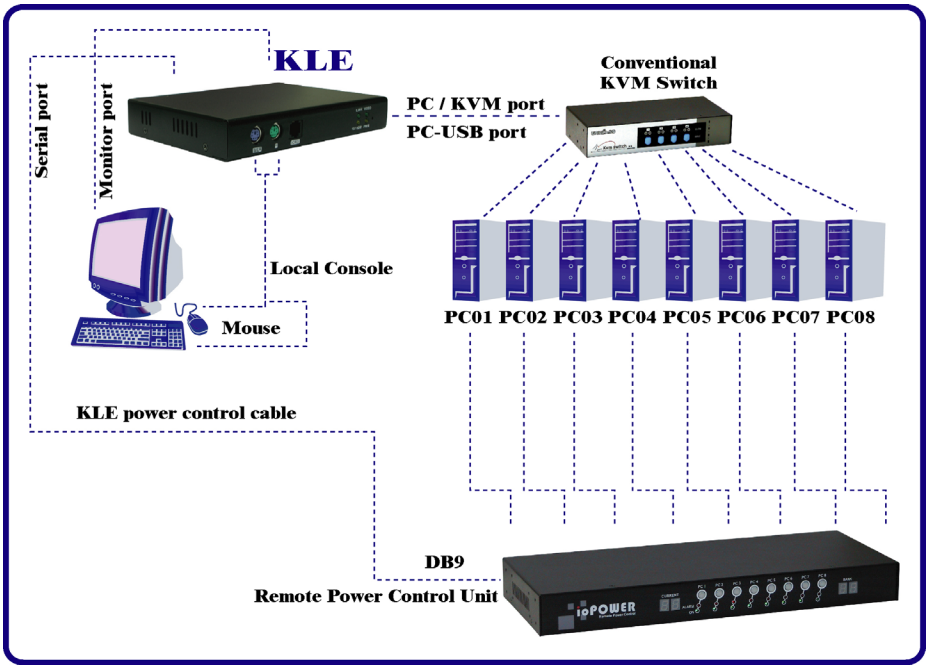


KLE connected to a single server



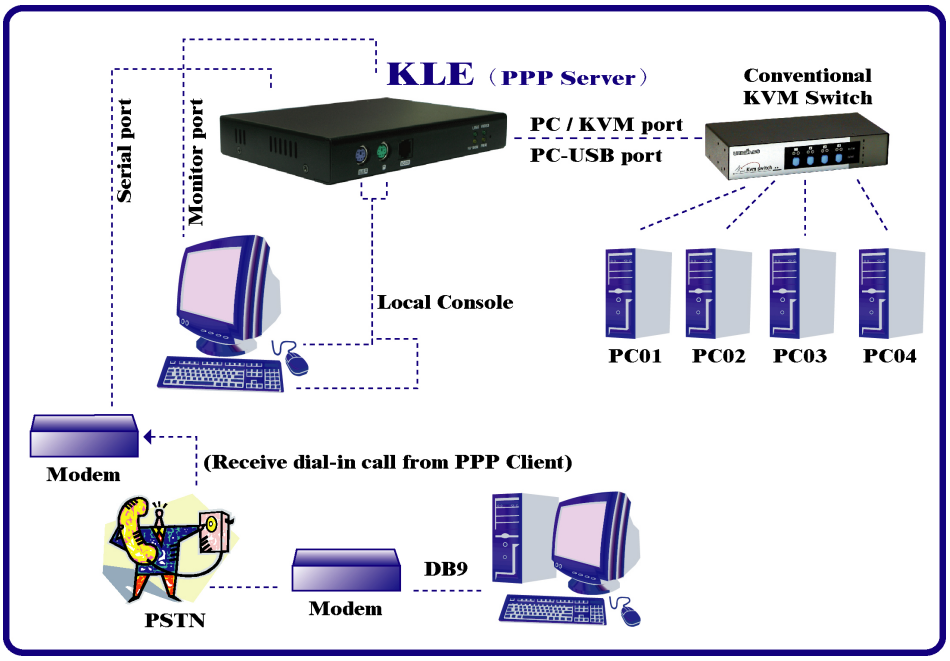
KLE connected to a conventional KVM Switch and multiple servers

1.3.2 Power Control Configuration

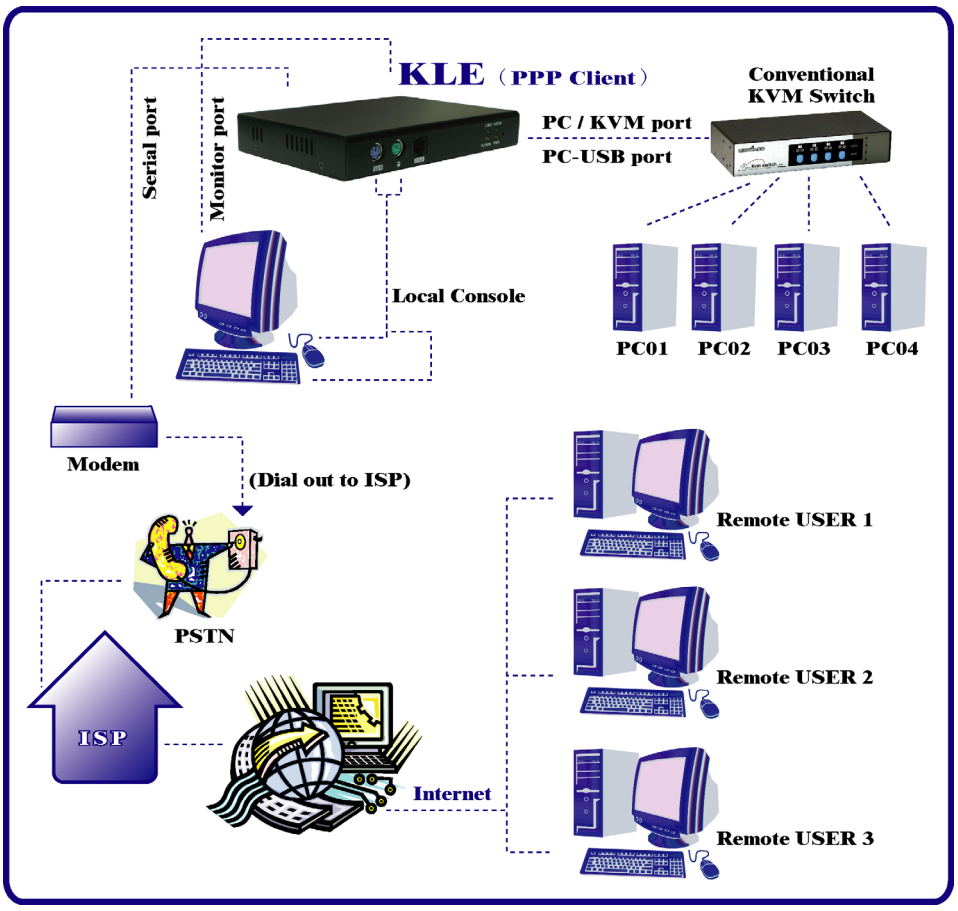


KLE connected to a Remote Power Control Device

1.3.3 PPP connections



KLE as PPP server to accept dial-in request from a remote PPP client via modem line



KLE as PPP client to dial-out to ISP for remote clients to access via the Internet

1.4 KLE External Views

1.4.1 KLE Front Panel

KLE Front-panel

PS/2 Keyboard port: This is where you connect the PS/2 keyboard for local console.

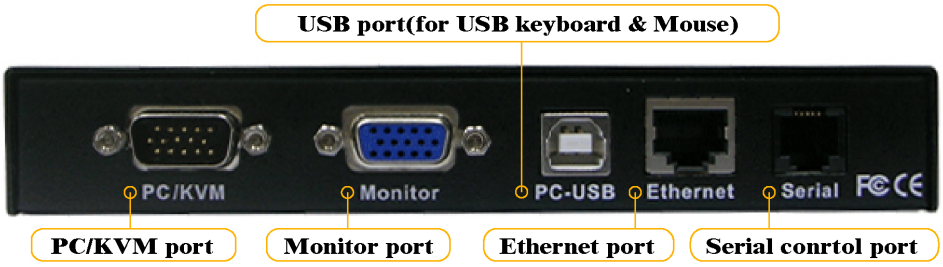
PS/2 Mouse port: This is where you connect the PS/2 mouse for local console.

Console Management Port (RJ-12): This is where you connect the serial console cable for advanced console management of KLE unit via a serial terminal emulation utility such as Windows HyperTerminal.

Status LED's
The 10/100Mbps LED is lit as solid orange when the current digital link is running on 100Mbps speed.
The Link/Act LED gives off solid green light when a network link is established and flashes whenever network transmission are perceived on the digital port.
The Power LED indicates the Power On status when it is lit as solid green.
The Video LED indicates the normal functioning of video server when it is blinking.

Restore-to-Default Button: The Restore-to-Default button is a tiny recessed button located to the right of the LED indicators, and can only be accessed by prying down with a pointed needle tip.
To depress the recessed button for over 4 seconds, and upon release, it will restore KLE to factory default – the default IP settings and user account settings that come with factory default settings.

1.4.2 KLE Rear Panel



KLE Rear Panel

PC/KVM port (HDB-15, integrated with PS/2 Keyboard and mouse signals): The PC port connector is where you should connect to either a single PS/2 computer or a single PS/2 KVM Switch, using the 3-in-1 slim KVM cables w/ an integrated HDB15 connector. However, if you are using USB-enabled computer or USB KVM Switch, you should additionally use a USB cable to connect to a USB port on your computer for keyboard/mouse connection.

Monitor Port (HDB-15): This is where you should plug in the Monitor for your local console on KLE.

USB port (USB Type B): This USB port provides USB keyboard/mouse connections to a USB-enabled PC, or to a USB KVM Switch. Thus, if you are connecting any USB-enabled PC or USB KVM Switch, please use a USB cable to make the connection.

Ethernet Port (RJ-45): The Ethernet port, or digital port, offers anytime anywhere access of KLE and subsequently the conventional KVM Switch (es) and servers/computers connected behind it to the remote login clients lover LAN/Internet.

Serial Control Port (RJ-12): The serial control port allows you to connect to either an external modem or a power control unit or to a cascaded chain of power control units. When added with an external modem to its serial control port, KLE could serve as, either a PPP server to allow direct cable connection, or dial-in connection from its peer computers, or as a PPP client to dial-in to the ISP or an enterprise PPP server. Furthermore, through serial commands sent over its serial control port, KLE can perform remote power on/off and power cycling task via the (cascaded) power control module(s).

1.4.3 KLE Power Socket

You should use the DC9V 2A Adapter provided within the package. Use of any other adapter will nullify the warranty.

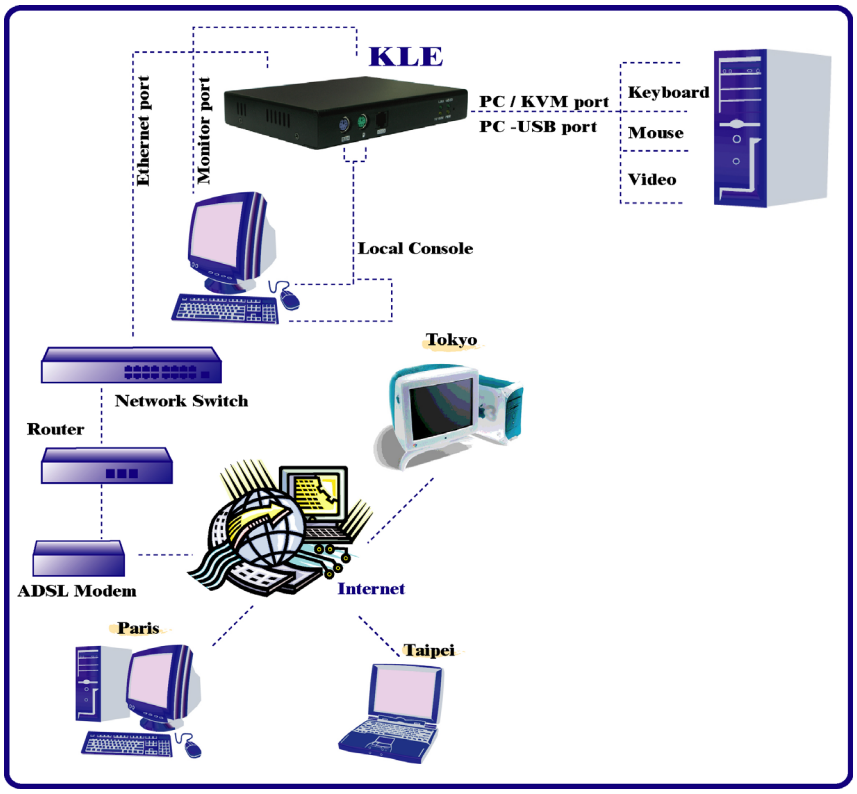
Chapter 2
Installing KLE

2.1 Physical Connections

Step 1. Power on the KLE: Connect the KLE Power adapter and power on KLE.

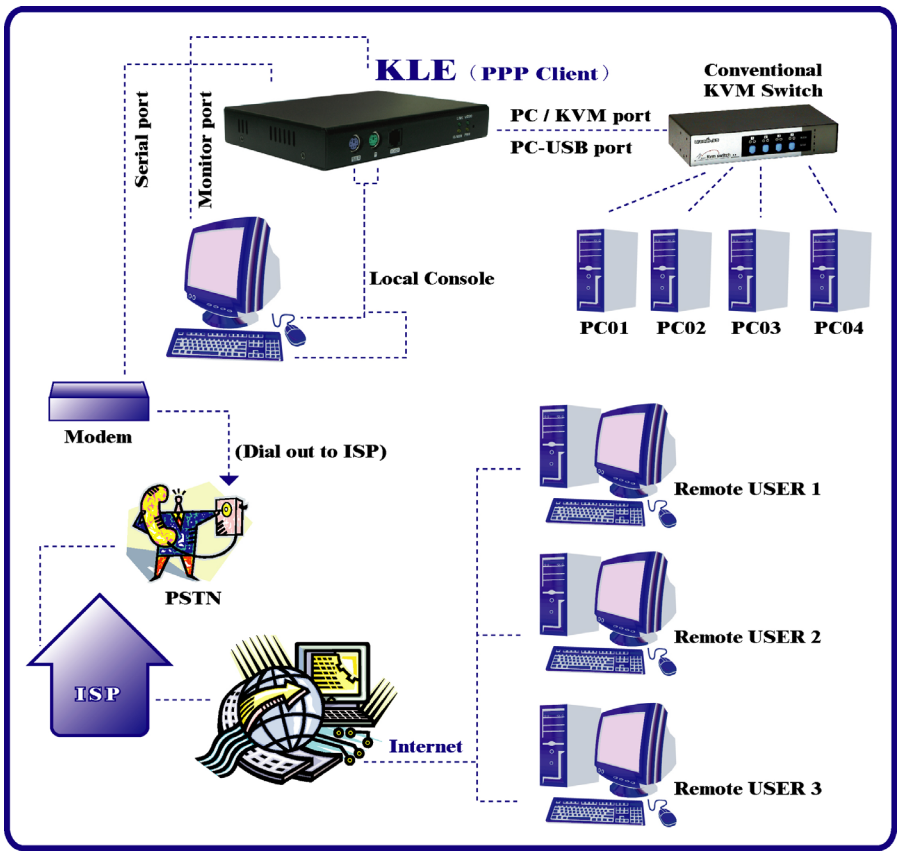
Step 2. Set up a local console on KLE: If a local console (that is a physical keyboard, mouse and monitor connected to the KLE) is required, connect the keyboard and mouse to the KLE local console ports (that is keyboard, mouse and monitor port specifically).

Step 3-a. Single Server Mode: If you need to connect to only one computer/server. Just connect to the PC/KVM port directly to the PC, using the 3-in-1 Slim KVM combo cable and/or the USB cable that come with the KLE packing box.



KLE configuration – Single server mode

Step 3-b. Multiple Server Mode: If you need to connect to multiple computers/servers, you should use a KVM switch in between the KLE and your connected computers/servers. Just connect to the PC/KVM port o the console port of your KVM switch using the 3-in-1 Slim KVM combo cable and/or the USB cable (if it is a USB KVM switch) that come with the KLE packing box. And the KVM switch will in turn be connected to the multiple computers/servers.



KLE configuration – Multiple server mode

Now that you have set up your local console on KLE, you can now configure your connected servers just by using the ready access provided by KLE's local console.

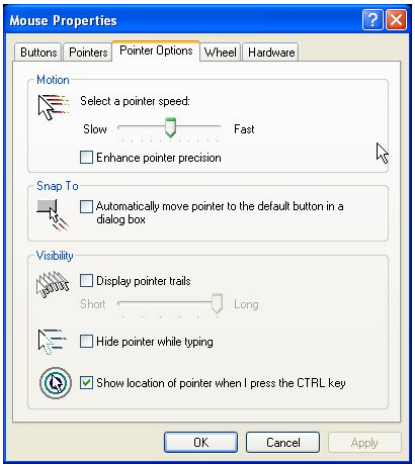
2.2 Configure Your Servers for Connections to KLE

Mouse acceleration is not supported in KLE. Therefore, you must turn off the mouse acceleration on all your connected servers.

2.2.1 Turn off mouse acceleration & "Snap to" option

Windows XP Platform
Access Control Panel/Mouse. On the Mouse Properties tab, select the *Pointer Options* page :

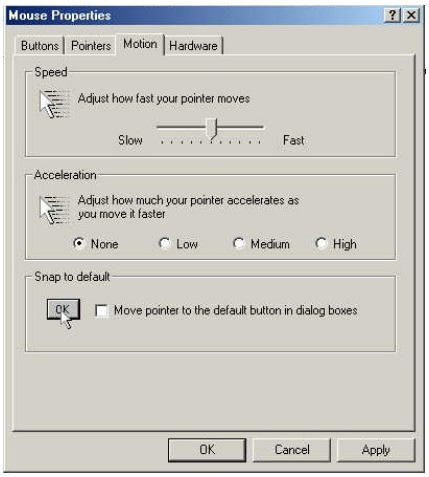
1. Adjust the pointer speed to the exact middle.
2. Uncheck the Enhance pointer precision option.
3. Uncheck the Automatically move pointer to the default button in a dialog box



Click *OK*.

Windows 2000 Platform
Access Control Panel/Mouse. On the Mouse Properties tab, select the *Pointer Options* page :

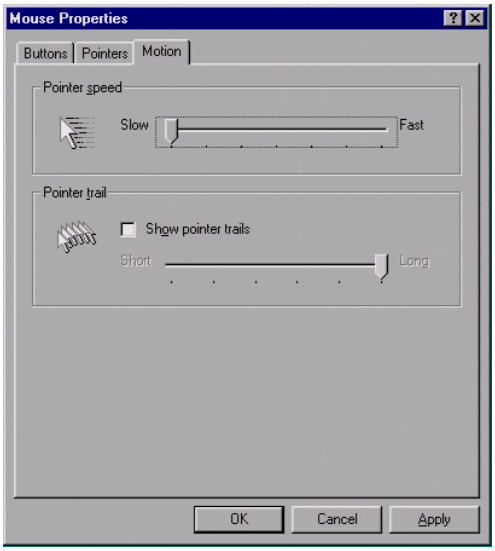
1. Adjust the pointer speed slide bar to the exact middle
2. Select the Acceleration as None
3. Uncheck the Move pointer to the default button in dialog box



Click OK.

Windows 98

Access Control Panel/Mouse. On the *Mouse Properties* tab, select the *Motion* page. Under the *Pointer Speed* category, adjust the pointer speed to the slowest (leftmost) position.



Click OK.

The mouse setting page on different Windows platforms might be quite different, some gives mouse acceleration option and some do not. If you see any mouse acceleration option, please uncheck it. If there is no mouse acceleration available on the setting page, you can adjust the mouse speed to either x1 or the slowest position (such as on Linux platforms). Sometimes, it requires a middle position on the speed slide bar to make mouse synchronization on the viewer side, for example, Windows XP requires a middle position on mouse speed. Anyway, the worst case is that you have to make some trial and error to make your mouse acceleration off and the speed as x 1 (could be at the slowest position or the middle position).

2.3 More Tips for Server Desktop Configuration

Several aspects have to be taken into consideration and maybe configured on your computers or servers for best performance:

(1) Resolution modes should refrain from too much peculiarity and better adopt ones that are within KLE's standard support.
(2) Turn off the Menu special transition effects on your operating system (especially on Windows XP, if you are using any) such as fade for best video refreshing effect, especially when you are using Medium or Low Video Quality as your video filter setting on KLE.
(3) Adjust the server desktop backgrounds as containing preferably plain, solid colors with simple designs (only for improving video refreshing speed when bandwidth is critically limited. No need to do so when bandwidth is ample)

2.3.1 Configure the display resolution on your server

KLE supports most display modes up to 1600 x 1200. However, you might encounter some display problems when your display card is outputting an unusual display mode. These possible problems are either no video or abnormal display on viewer screen.

To simplify the display factor before connection to KLE, we suggest you use more standard display modes such as: 800 x 600 @ 60Hz/72Hz/75Hz, 1024 x 768 @ 60Hz/72Hz/75Hz, 1280 x 1024@60Hz, 1600 x 1200@60Hz, etc. For the suggested display modes, please refer to the following table.

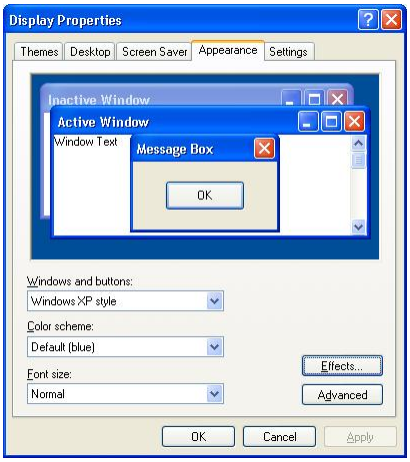
	640 x 400	640 x 480	800 x 600	1024 x 768	1152 x 864	1280 x 1024	1600 x 1200
56Hz							
60Hz		✔	✔	✔	✔	✔	✔
61Hz							
64Hz							
70Hz	✔			✔	✔		
72Hz		✔	✔				
74Hz							
75Hz		✔	✔	✔			
76Hz				✔			
78Hz					✔		
84Hz							
85Hz	✔	✔	✔	✔			
100Hz		✔	✔	✔			

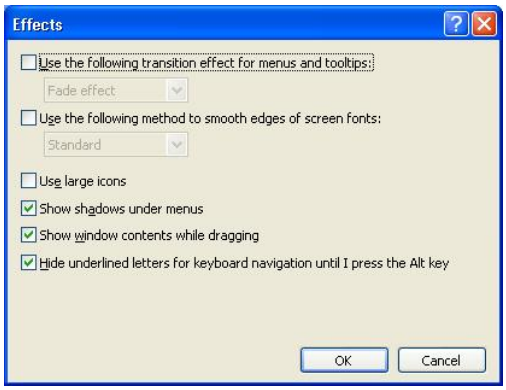
Note: These are suggested display modes for server desktop connected KLE. However, the actual feasible display modes for as specific server desktop will be dependent on its display card. Some display modes listed here might not be feasible with some display card. Try to do some trials to determine the best display mode for your desktop on KLE viewer.

2.3.2 Disable special transition effects on the screen outputs of your connected servers

Go to *Control Panel/ Display / Appearance / Effects*. Then uncheck the option to disable transition effects such as *Fade* for the menus and tool tips. You should perform the same check on each of your connected servers.

On Windows platforms such as Windows 98, 2000, XP and 2003 Server, some transition effects might yield undesirable video refreshing artifacts, especially when you are using Medium or Low Video Quality as your video filter settings. To avoid undesirable artifacts from appearing on your screen, please turn off the special transition effects.




Effects
Use the following transition effect for menus and tooltips:
Fade effect
Use the following method to smooth edges of screen fonts:
Standard
Use large icons
Show shadows under menus
Show window contents while dragging
Hide underlined letters for keyboard navigation until I press the Alt key
OK
Cancel

2.3.3 Choose plain and solid server desktop backgrounds for your connected servers.

To optimize the bandwidth efficiency and speed up video performance across bandwidth-limited environment, one should preferably adopt a server desktop, which should be as plain as a color background with a solid and light-colored graphics. Complex patterns or color gradients should be avoided, if bandwidth is critical in your application, since they will create more bandwidth demands for their transmission across the Internet.

2.4 KLE Network Settings

2.4.1 IP Settings

The factory network settings for KLE are as follows:
IP address: 192.168.1.200
Net mask: 255.255.255.0
Gateway: 192.168.1.254
DNS: 192.168.1.254

Step 1. Connect your KLE to the Ethernet LAN.
Step 2. Access the KLE web management interface by typing the following in the address bar of your browser window on a remote client:

https://192.168.1.200:5908

Step 3. Then a login prompt will ask you for the account name the password. Use the default account and password:
User Name: superuser
Password: superu

After logging in, you will see the KLE Web Browser Management Interface.

Step 4. Go to the LAN TCP/IP page on the **KLE** Management Interface and modify your IP settings. Refer to *Section 4.6 , Main/TCP/IP Settings – Port and IP Settings.*
Step 5. Apply the new setting by clicking *Apply Settings*.

to verify the **KLE** network connection, try to open the **KLE** web management Interface using the new IP address. Note that the IP address should be followed immediately by a colon and the port base +8 for port number,

https://<IP_address>:<PortBase+8>.

For example, if the IP address is 192.168.1.7 and the port base number is 5900, then you should enter

https://192.168.1.7:5908

Remember that it's a secure SSL encrypted connection, so you should type "https" instead of the

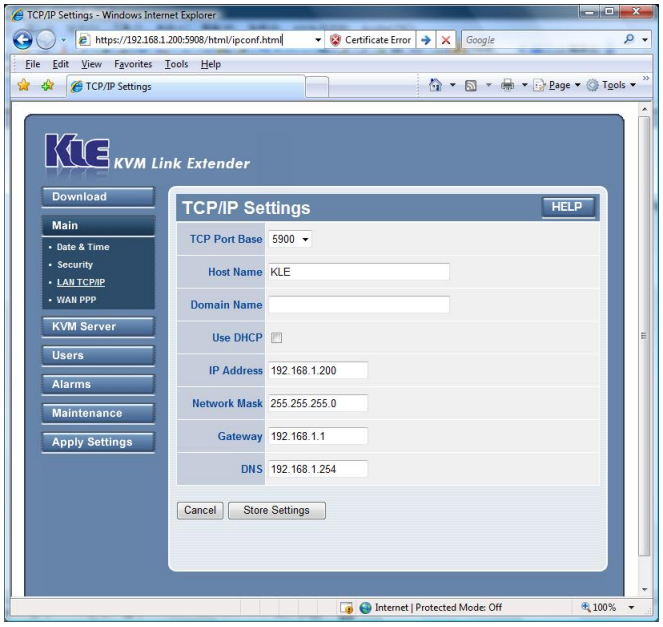
usual “http”. Otherwise, the connection will not be established.

2.4.2 Port Base

If you are satisfied with the default port base as 5900, you can skip this section. The default port base for KLE connection is set at 5900. This means it will use port 5900 (port base) for viewer connection and port 5908 (port base + 8) for https web browser connection.

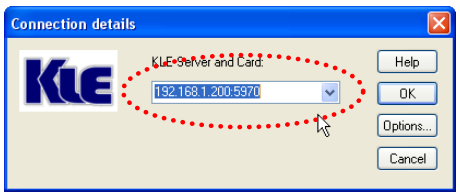
<Port base> – used for viewer connection
<Port base + 8> – used for secure browser connection

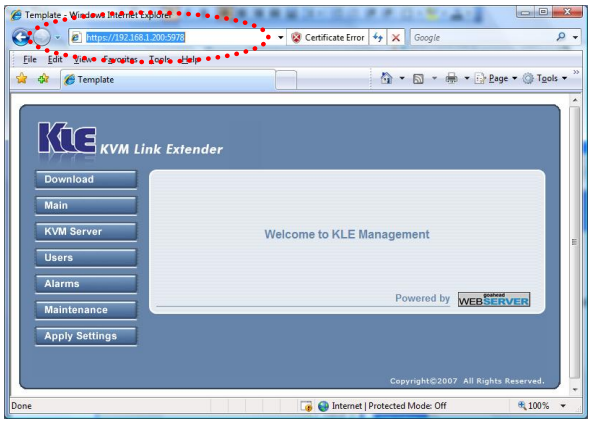
However, if you intend to use your own port base setting, just access the web management interface and configure the port base as following:



For example, if you choose 5970 as your port base, then you have:

5970 – used for viewer connection
5978 – used for secure browser connection





Click *Submit* and *Apply Settings* to validate your new setting.

Now you have installed **KLE** within your Local Area Network environment, and can try to establish a remote viewer connection…

2.5 Configuring your Firewall and Router for Accessing KLE across the Internet

To allow access to the KLE behind corporate firewall/router, please set up your firewall/router (not your KLE) as following:

Step 1. Configure a virtual server on your router: you should configure (or ask your net admin to configure for you!) a virtual server as mapped to the KLE local IP address.

Step 2. Open a port range: (<port_base> ~ <port_base_+_9>) both inbound and outbound for the virtual server: you should open a port range according to what you have configured as port base for KLE previously.

Taking previous example, if we configure KLE as having a port base of 5970, then we should open port range 5970~5979 (that is, <port_base> ~ <port_base +9>) both for inbound and outbound, in which,

<port_base> = 5970 is the KLE viewer connection port
. . . . . .
<port_base + 8> = 5978 is the browser SSL connection port
<port_base + 9> = 5979 is for viewer internal communication, etc.

For example:
Router internet IP ←→ virtual server (port range open) ←→ KLE local IP
61.232.134.120 ←→ virtual server (port 5970~5979 open) ←→ 192.168.1.7

Once you haved configure a virtual server with appropriate port range open (<port_base> ~ <port_base_+_9>), you can then try to access your KLE across internet by using in the public IP address and designated port number. For example, in this case, we have

Browser access: https:// 61.232.134.120:5978
Viewer access: 61.232.134.120:5970

If you have domain name mapping to the public IP address, you can also use the domain name, for example:

Browser access: https:// www.mycompany.com:5978
Viewer access: www.mycompany.com:5970

Once you have changed the port base of your KLE, you should also modify the open port range on your router accordingly, if you want the Internet access to come across.

2.6 Security Settings

There are altogether nine (3 x 3) possible combinations of Viewer Security Levels + Password Policies that are available for a flexible adaptation to your security needs. The administrator can choose an optimized combination of user password policy and SSL/PKI Authentication according to his security and convenience concerns.

	User Password Policy		
SSL / PKI Authentication	No password	Global Password	User-specific Password
No SSL-No PKI	N – N – N	G – N – N	U – N - N
SSL – No PKI	N – S – N	G – S – N	U – S - N
SSL - PKI	N – S – P	G – S – P	U – S - P

G – Global Password U – User-specific Password
S – 256-bit SSL Encryption
P – 1024-bit PKI Authentication
N – Not available

Open the Security page of the KLE web management interface.

2.6.1 Select a User Password Policy

KLE offers three types of password policies.

1. No Password
2. Global Password
3. User Password

No Password: the viewer does not prompt you for any password. Anyone who has a viewer and passes the security level check of the viewer can establish the connection.

Global Password: the viewer prompts you for a global password, which is used by all who want to make viewer connections to KLE.

User Password: the viewer prompts you with user-specific password. With this setting, each login user is checked against his or her corresponding password before allowing viewer connection.

Click Store Settings to validate your selection. Go to the Apply Setting page and click the Restart Server button to apply your settings.

2.6.2 Select a Security Level for Viewer Connection

There are three security levels for choice:

- Level 1: No encryption (No SSL)
- Level 2: 256-bit encryption, no user certificate required for user authentication
- Level 3: 256-bit encryption, user certificate required for authentication (PKI)

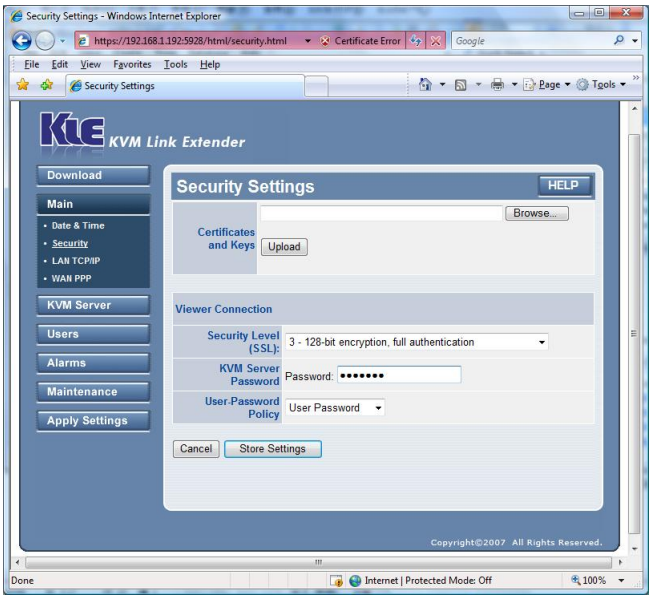
Security level 1: provides no security and must be reserved for internal LAN connections.

Security level 2: provides usual secure SSL connection with encryption for mouse, keyboard, and video, but uses no PKI-authentication. The viewer identifies that KLE is a KLE device and everything is encrypted with an ephemeral 256-bit key. The user authentication is based on a user name and password. It is the recommended default security level. It is flexible because you can connect to KLE from any computer, provided you know your user name and password.

Security level 3: offers a secure SSL connection with encryption for mouse, keyboard, and video, and uses 1024-bit PKI-authentication. It should be reserved for very high security applications. It is based on certificates and 1024-bit RSA keys. The individual keys are protected by passphrases that come in addition to user passwords. The viewer identifies the KLE certificate and KLE identifies each user certificate. Special sets of PKI certificates and keys must be installed into KLE and into each computer that wants to connect to KLE. Normally, each user is given a proprietary certificate and he is the only one who knows the passphrase. This mode is highly secure but a little bit constraining for users. As a user, you must install your certificate into the computer(s) you will use to access KLE. You must type you passphrase each time you login. This passphrase cannot be filled out automatically by the viewer or the browser.

The choice of a security level to be implemented for the KLE viewer connection is of most importance, especially when your remote server connections require high security to keep your servers safe from unauthorized entries and/or network sniffers.

If you choose to implement the PKI authentication feature, select *Level 3 viewer security connection* on the *Security* page.



Into *KVM Server Password,* enter the password for the server private key serverkey.pem (`serverpwd` for the set of certificates provided on the Support CDROM). Refer to next section for more information about KLE certificates.

Click *Store Settings* to save your settings and go to the *Apply Settings* page to make them active.

2.6.3 Installing Certificates and Key on KLE for Security level 3

You don't need to install any certificate unless you plan to use the security level 3 (refer to previous section). You can skip this section if you plan to use the security level 1 or 2.

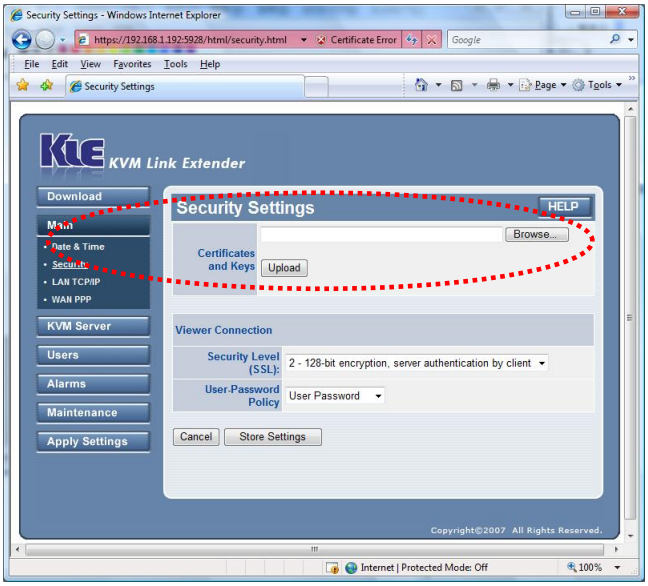
You can use the default set of certificates (provided on the CD-ROM) for training. However, it is not recommended to work with these certificates because anybody who has got a copy of them might establish a connection to your servers. Therefore, we recommend you obtain your own certificates from a public Certificate Authority or you generate a private set by using some CA software such as XCA.

For certificate generation and certificate characteristics, please refer to "How to Generate KLE Certificates using XCA" (can be found on the KLE support CD-ROM).

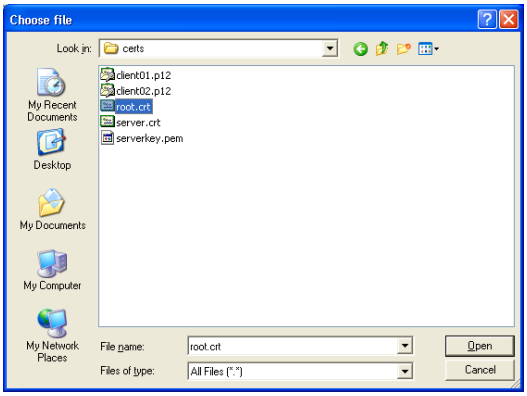
Certificate and key files to be installed on KLE:

(1) The root certificate: root.crt
(2) The server certificate: server.crt
(3) The server private key: serverkey.pem

Open the *Security Settings* page of the KLE Management Interface.



Step 2: Click the *Browse* button and use the *Choose File* dialog box to browse to your certificate files.



Step 3. Click Upload to upload the root certificate to KLE. After the uploading is completed, you can see the prompt page for reboot.

Click Reboot and wait until KLE is booted up. Then try to import the server.crt and the serverkey.pem files.

You do not have to reboot after each certificate. You can do one complete reboot at the end when you finish uploading all of them. To return to the *Security* page instead of rebooting, click the *Security* page hyperlink on the left frame.

2.6.4 Remote Clients

Depending on your security settings, you have to distribute some files and/or pieces of information to the remote clients:

1. Certificates: as you have obtained from your CA (Certification Authority). They are required only if you select level 3 viewer security

- root.crt
- client_name.p12. (client_name is freely chosen)

2. Client Certificate Password: as you have obtained from your CA. It is required only if you select level 3 viewer security. (clientpwd if you use the default set of certificates provided on KLE CD-ROM)

3. User Name and Password: as you have specified in the *User Management* page. It is required only if you choose *User Password Policy*. By default, there are three users into KLE user database:

	Name	**Password**	**Privileges**
1	superuser	superu	Super administrator
2	admin	123456	Administrator
3	user	123456	Simple user

4. Global Password: as you have specified in the *Security Page*. It is required only if you use the *Global Password Policy*.

Chapter 3
Viewer Connection

KLE provides a win32 viewer for Windows clients and a Java viewer for cross-platform on any major operating systems.

3.1 Installing the Viewers on the Client Computer

3.1.1 Win32 Viewer

Go to the *Download* page to download the Win32 viewer, Kripview_install.exe. Install the viewer program on the client computer that will connect to KLE. After installation, a desktop icon will be created on your client desktop.

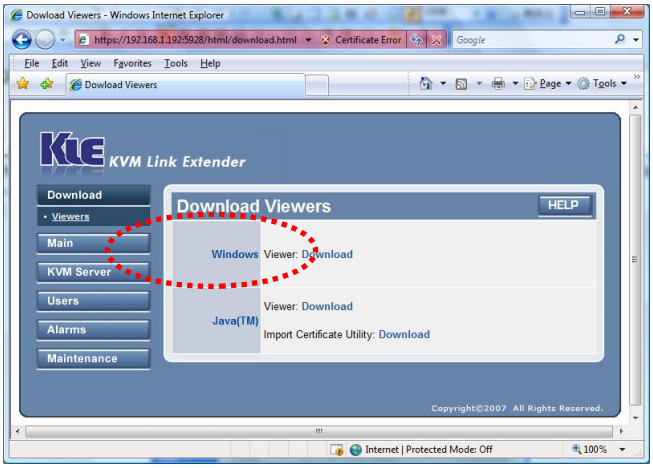


Figure 1: Download Page

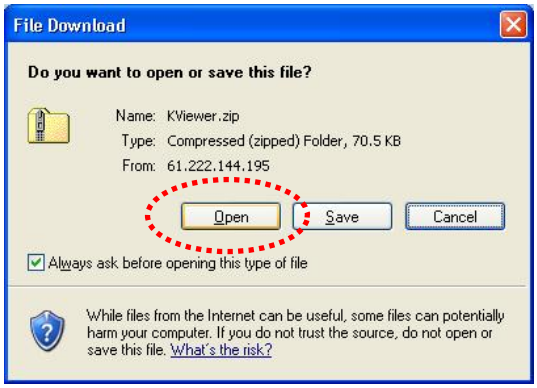
3.1.2 Java Viewer

Before you can use the java viewer, you should first install the Java Runtime Environment, JRE 1.5.0 or higher, which is downloadable from http://www.java.com.

To open the Java viewer, go to the *Download* page of the web management and click *Download*.

If the .jar file association is correctly done on your computer, choose to open it directly.

Otherwise save the KViewer.jar file to your local hard disk and then type "java -jar KViewer.jar".


File Download
Do you want to open or save this file?
Name: KViewer.zip
Type: Compressed (zipped) Folder, 70.5 KB
From: 61.222.144.195
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

3.2 Installing Certificates on the Client Computer

Skip this section if you are not using the security level 3 (refer to section 2.6.2).

To make full PKI authenticated viewer connection with KLE, you need to import client certificates in .p12 format to the client computer. You can use the default client certificates provided on CD ROM or (recommended) your own set of certificates. Each viewer provides a utility for certificate importation.

Note: the win32 viewer and the java viewer require separate certificate importation to get the job done. If you plan to use both viewers on the same machine, you will have to import the certificate twice, once with each viewer certificate utility.

3.2.1 Win32 Viewer

Run the importation utility by accessing Start/Programs/PROSUM /KLE Viewer/Import Certificates. Click on *Root Certificate* to import the root certificate, and then click on *Client Certificate* to import the client certificate.

3.2.2 Java-based Viewer

Run the Java importation utility Impcert.jar by typing

java -jar Impert.jar

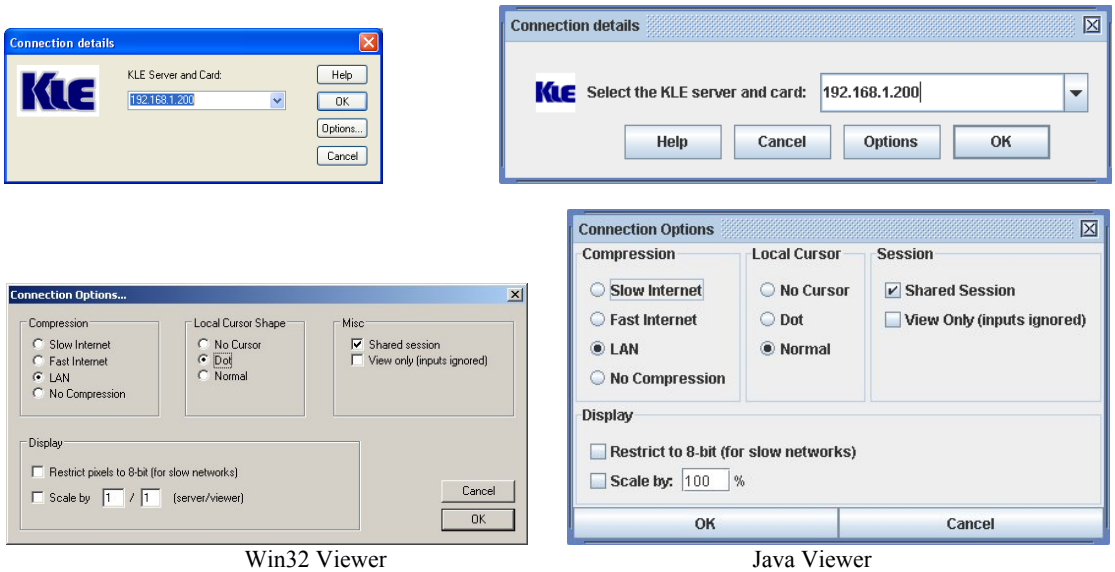
Click on *Root Certificate* to import the root certificate, and then click on *Client Certificate* to import the client certificate.

3.3 Starting the Viewer Connection

3.3.1 Specifying the Viewer Connection Options

The viewer *Connection Options* interface provides several alternative options to optimize your viewer connection.

Click the *Options* button on the *Connection Details* dialog box.



Win32 Viewer Java Viewer

Encoding

Slow Internet:	Video quality is optimized for viewer connection with slower Internet bandwidth
Fast Internet:	Video quality is optimized for viewer connection with better Internet bandwidth
LAN:	High video quality for viewer connection over LAN
No Compression:	Best Video Quality with no compression, but poor performances

Local Cursor Shape

No cursor:	Local cursor invisible on KLE Viewer
Dot:	Dot shape for local cursor on KLE Viewer
Normal:	Arrow shape for local cursor on KLE Viewer

Misc

Shared Session:	Multiple users access same server desktop
View Only:	Keyboard and mouse inputs are ignored (not restricting keyboard and mouse access on other users).

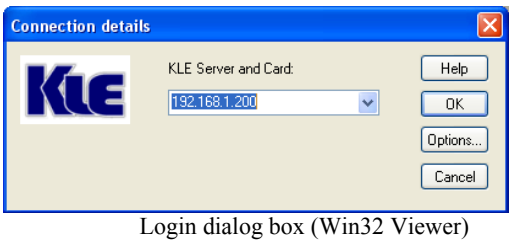
Display

Restrict to 8-bit:	Color reduction to 256 colors for slow connections
Scale x/y:	Scale the display output on viewer (not affecting the actual transmission bandwidth)

3.3.2 User Name and Password

First, run the viewer program, enter the access IP and port number for KLE.

Default IP address: 192.168.1.200



Login dialog box (Win32 Viewer)

At the password or private path phrase prompt, just enter the user name and password as required:

Default user & specific password:
User: superuser
Password: superu

Or, if you are using the Global Password policy setting …

Default global password: 123456

Or, if you are using the Level 3 security setting that requires installation of certificates for PKI authentication (For details, please refer to Section 4.5 , Main/Security –Certificates Installation, Viewer Encryption and Password Policies.)

Default private path phrase: clientpwd

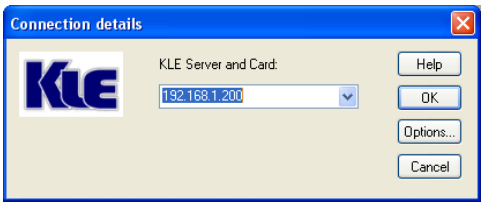
After you have entered the global password, user name and password, or private path phrase as its security and password policy require, a viewer connection will be established successfully.

3.4 Some Tips about Viewer Connections

3.4.1 Typing the KLE IP Address

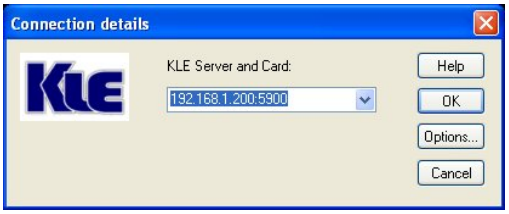
If you want to specify the type of connection rather than using the default one, click the *Options* button and optimize your connection parameters. Please refer to previous section for details.

Note that you can simply type in the access IP address of KLE server without specifying the port number when the port number is 5900 (default value).




```
IP_address [only if port number is 5900]
192.168.1.200
```

Of course, you can always type




```
IP_address:port_number
192.168.1.200:5900
```

However, if the port setting on KLE is already changed to another port number, you have to specify its specific port number following the IP address. For example, if you want to connect to port 5910 on the KLE server, type:

```
192.168.1.8:5910
```

To configure the port base number, please refer to Section,4.6 ., Main/LAN TCP/IP – Port and IP Settings.

3.4.2 Connection Performance Tuning

If you are using a dial-up modem line and experiencing slow keyboard mouse movement and response, you might check whether you are using the default LAN encoding scheme or even the *No Compression* scheme, which requires much more bandwidth; or there is a network bottleneck somewhere in between KLE and your client desktop. For more details, please refer to Section 3.10 , Common Video Display Problem Troubleshooting.

3.4.3 Local and Remote Mouse Cursor Synchronization

Normally, you will see both the local cursor and the remote cursor on the view area. You can specify the shape of the local cursor as seen within the viewer window either as a dot, an arrow or none (not showing any local cursor within the viewer area). Also if these two cursors become out of sync, all you need to do is to hit the mouse synchronization hotkey - by default (right) Ctrl / (right) Ctrl / Home - to synchronize the two cursors.

Mouse cursors out of sync

Local/remote cursor resynchronization default hotkey: RCtrl-RCtrl-Home

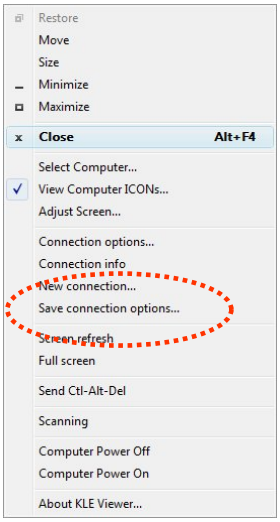
Mouse cursors in Sync

While operating your mouse, it is not necessary to wait until the remote cursor has actually caught up with the local one before you can click on the target in the view area. Actually, you can click the target just using the local cursor without waiting for the remote cursor, because the click point is recorded and the click will always take place at the right location. Therefore, if both cursors are synchronized, the important one is the local cursor. You need not care about the remote cursor. That is why we recommend you always choose the biggest local cursor in viewer settings.

3.5 Saving the Connection Options

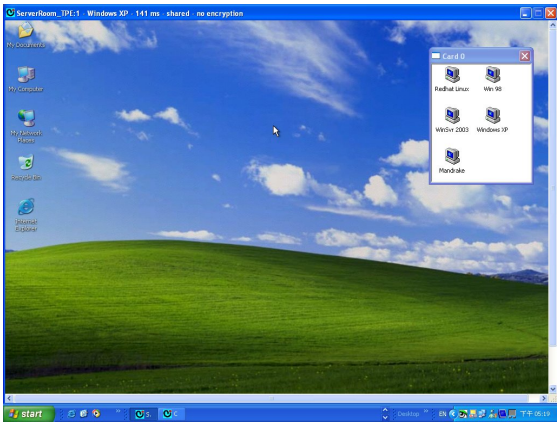
After you have optimized your connection options, you might want to save them. Next time when you log in with the viewer to the KLE server, the viewer on that specific client computer will use the saved connection parameters as well as the password (but not the private path phrase, which is not saved since it is used by secured/PKI-authenticated connection) for connection with KLE.

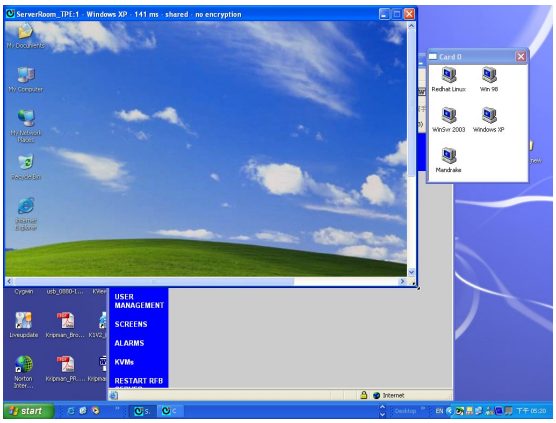
To save connection options, click the KLE icon on the Viewer title bar to open the viewer Quick Menu and select *Save* the connection options.



KLE Viewer Quick Menu (Win32 viewer)

3.6 Adjusting the Viewer Window Size



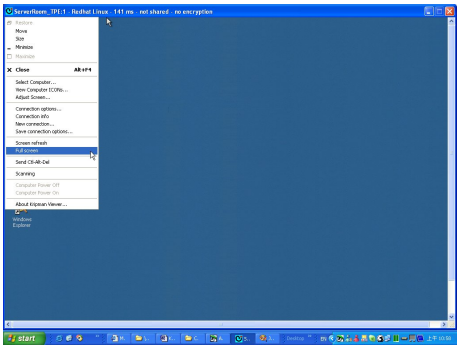


Viewer Window with scroll bars (Win32 viewer)

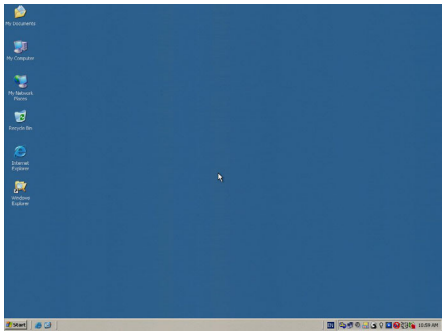
The size of the KLE viewer window can be adjusted by dragging the border of the viewer windows.

3.6.1 Changing the Viewer Size to Full Screen (Win32 Viewer only)

1. Select the Full Screen option on the Quick Menu



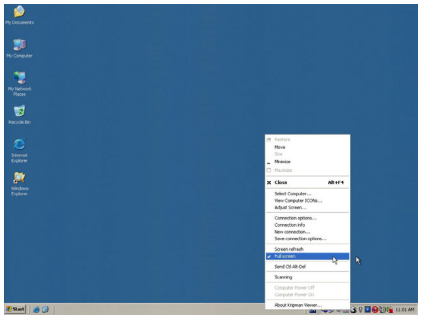
2. Click *OK*, and the viewer goes to full screen mode.



3. A message box appears to remind you how to exit the full screen mode

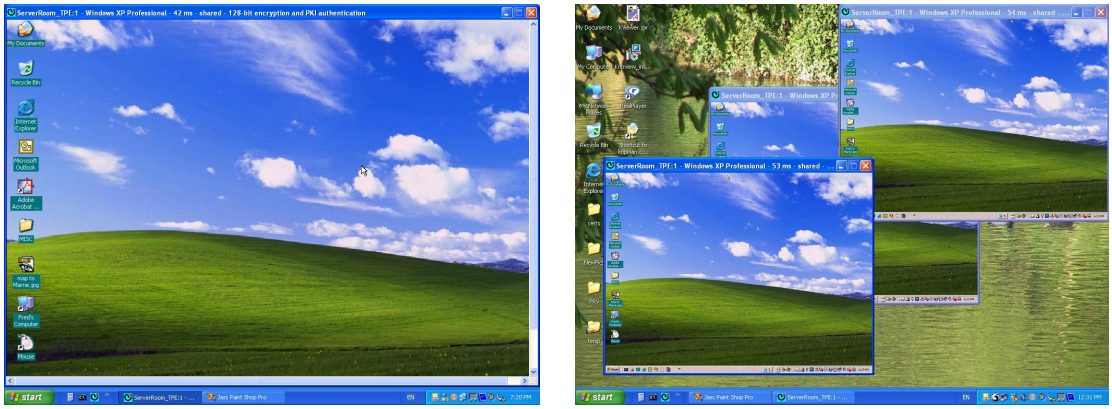
Kripman viewer full-screen mode
To exit from full-screen mode, use Ctrl-Esc Esc and then right-click on the Kripman viewer taskbar icon to see the menu.
OK

To exit the full-screen mode, just hit Ctrl-Esc to bring up the local task bar. Right-click the viewer taskbar icon to bring up Quick Menu, then click to deselect the full screen mode to restore it to window mode.



3.6.2 Scaling the Viewer Window

Click the KLE viewer icon on the title bar of the viewer window to evoke the Quick Menu. Select Connection options on the Quick Menu

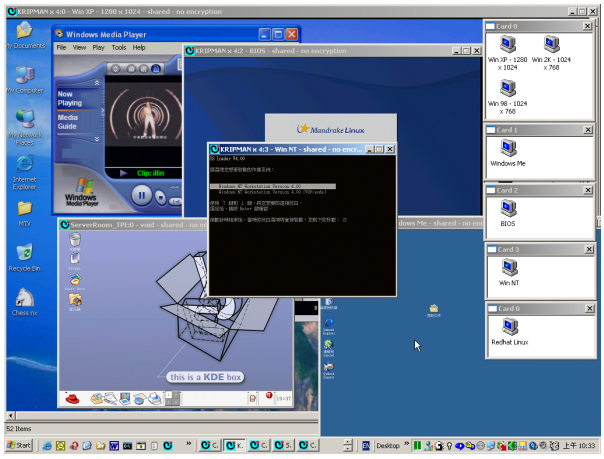


Scale the viewer window to ½ size

On the *Connection Options* dialog box, specify the preferred proportions of the viewer window, for example: ½, and then check the option. Click *OK* to scale the window to half size.

3.6.3 Centralizing the control of your remote servers

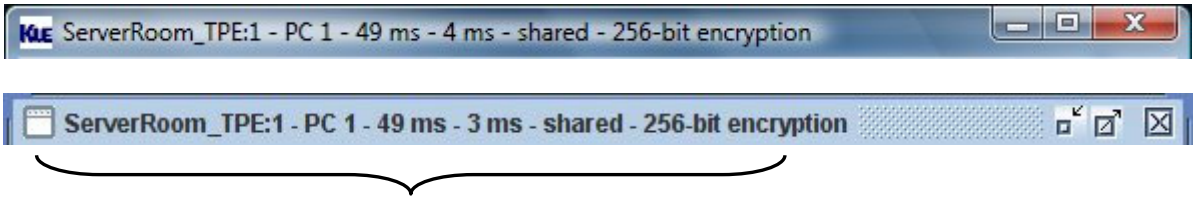
If you have multiple KLE units installed in a distributed manner among your global branch offices, you can then simultaneously monitor different remote servers distributed over this IP KVM Link Extender infrastructure on a single client desktop.



Five Win32 viewers on a Windows client desktop
(each showing one different remote server desktop)

Four Java Viewers on a Linux client desktop
(each showing one different remote server desktop)

3.7 Viewer Title Bar Information



Connection Information shown on the Title Bar

ServerRoom_TPE: This is the name you specified for your Video Server.

PC 1: This is the name you specified for this connected computer

49 ms: This is the capture time that is used for capturing the video image

4 ms: This is the transmit time that is used to transmit a video refresh

Shared: This is a shared session that allows other authorized users to login

Not shared: This indicates a non-shared session that blocks others from subsequent logins

No Encryption: This indicates no encryption for signal transmission (Level 1)

256-bit encryption: The current viewer session is using 256-bit SSL connection (Level 2 and 3)

PKI Authentication: The current viewer session is PKI-authenticated (Level 3)

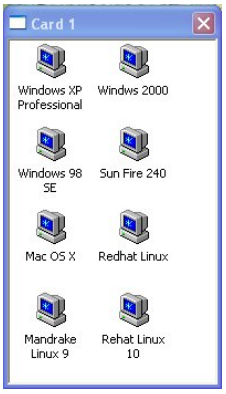
3.8 The Select Computer Box

3.8.1 Win32 Viewer

The *Select Computer* box allows the user to perform intuitive Click-and-Switch operation without memorizing the varying port-switching hotkey commands of all kinds of KVM switches possibly installed behind KLE. However, to use the click-and-switch feature provided by it, you must first configure the KVM switching hotkey commands for that KVM switch model via the web management Interface. Please refer to Section 4.13 , KVM Server/KVM Switch Database – Keeping and adding your KVM Data Base

The *Select Computer* box shows always on top of your screen once the KLE viewer connection is successfully made. On the box, you can see the computer icons together with the computer names you have already specified for each of them using the web management interface.

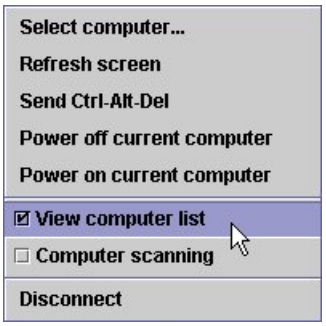
Click-and-Switch : To switch to a computer, just click a computer icon on the box.



Note that those computer icons represents only the computer names you have already registered using KLE Web management interface, not indicating any status of its connection such as whether it is in powered-on or powered-off state.

3.8.2 Java Viewer

To bring up the *Select Computer* box, click the *View Computer List* option on the Quick Menu. For the java viewer, the *Select Computer* box will not appear by default.

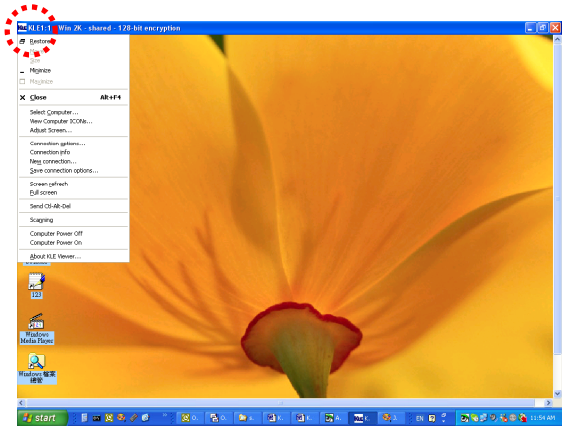


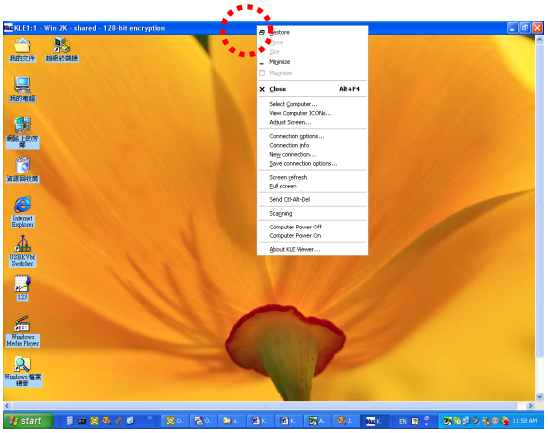
To switch to specific computer, just click any item on the listing …

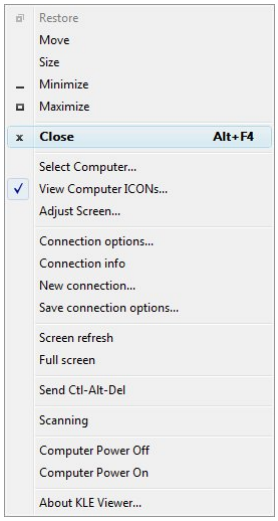
3.9 Viewer Quick Menu

3.9.1 Opening the Viewer Menu

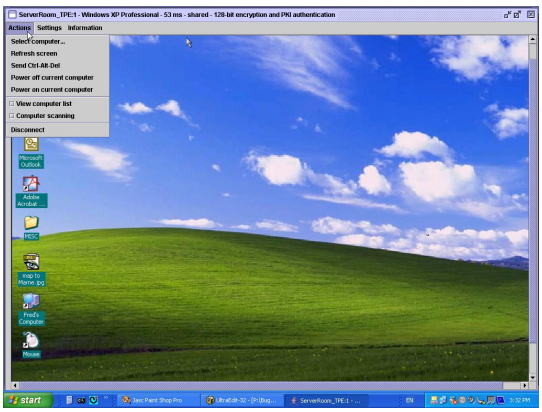
The *Quick Menu* of KLE's Win32 viewer can be evoked by clicking the program icon on the leftmost of the title bar, or right-clicking anywhere on the title bar.

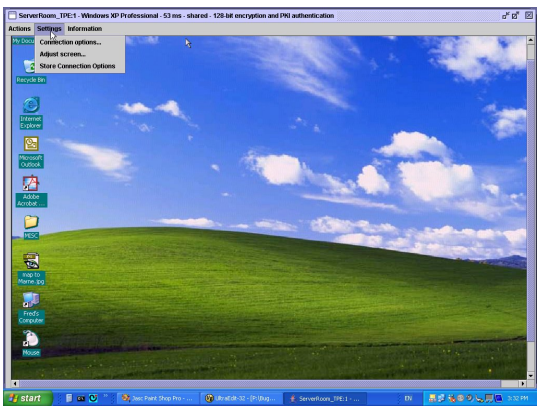






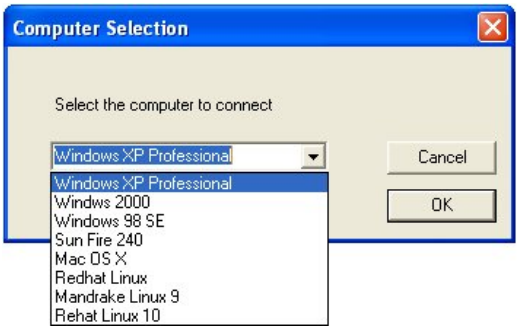
To open the Java viewer *Quick Menu*, click the menu options under the title bar.



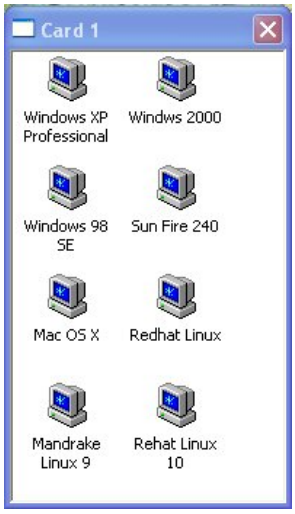


3.9.2 Menu Items

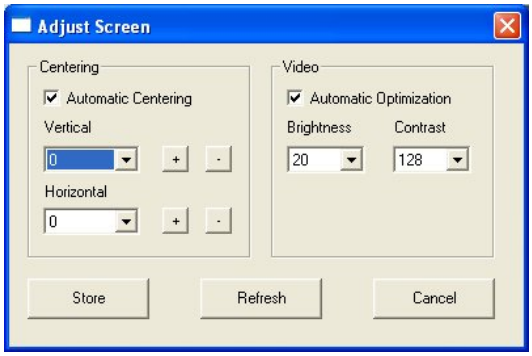
Select computer: Select the remote computer by a drop-down combo box



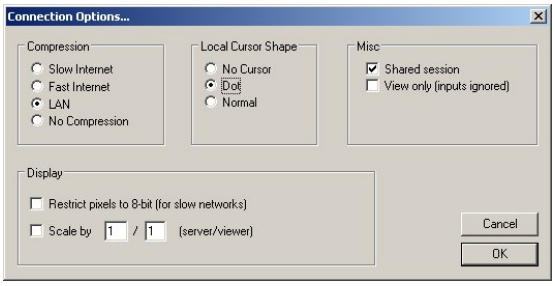
View Computer ICONs : Open the Select Computer box for computer selection by clicking icons



Adjust Screen: Fine-tune the screen area by pixel shifts.



Connection options: Open the Connection Options dialog box



Connection info: Show the Connection information of the viewer session.

KLE Server Connection Information
Connected to: KLE:1 - Win 2000 - 40 ms
Host: 192.168.1.200 port: 5900
Sharing option: shared
Encryption: 128-bit encryption
Desktop geometry: 1024 x 768 x 16
Using depth: 16
Frame capture period: 40 ms
OK

New connection: Make another new connection by the viewer.

Save connection options: Save the connection options settings such as those connection parameters specified within the Connection Options Box and also the password within the registry of the client computer. By selecting this option, you can save your session password as well as other connection parameters in the registry of your client computer, so that next time when you log in the viewer for a new session, you will not be prompted for session password again. However the client path phrase required in the connection of Level 3 security (256-bit SSL encryption and PKI Authentication) will not be saved and will be asked for every time when you login under Level 3 security setting.

Screen Refresh: Force updating of the viewer screen output

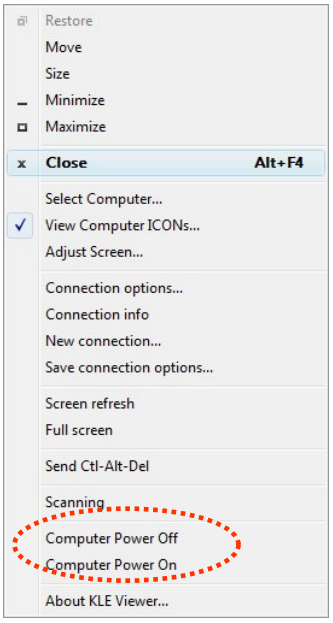
Full Screen: Change the viewer screen to Full Screen mode (Only the Win32 Viewer supports this Full Screen option).

Send Ctrl-Alt-Del: Send a Log On (Log Off) key sequence to the remote end.

Scanning: Start scanning through computers by issuing a programmable port switching commands with a delay time to a conventional KVM Switch behind KLE.

Computer Power Off: Send a Power Off serial port command to the remote power control unit (Only SUPERADMIN or ADMIN is allowed).

Computer Power On: Send a Power On serial port command to the remote power unit (Only SUPERADMIN or ADMIN is allowed) Power-on/off options grayed-out (unavailable for User privilege)



Now you have got yourself well familiar with KLE viewer interface, so go ahead to use and enjoy the remote viewer connection!

3.10 Video Display Problem Troubleshooting

KLE video server supports most major display modes up to 1600 x 1200. However, some display problems will occurs, when either there is abnormal or unusual display output from your server or the display resolution is over the biggest support of 1600 x 1200, or the display vertical frequency is beyond the support range in that pixel dimension.

To yield best video results on the viewer screen display on remote login client, you should also refer to Section 2.2 , *Configure your Servers for Connections to KLE*, and Section, 2.3 , *More Tips for Server Desktop Configuration* for more details about how to prepare your servers/computers before getting them connected to your KLE.

The followings are some common video display problems and their troubleshooting….

Q. There seems to be many artifacts or residuals not getting refreshed on the viewer screen. Is there any way to improve the video display quality on viewer screen?

A: The causes of these artifacts or residuals could be:

(1) The video filter currently active on KLE is either set at Medium Quality or Low Quality Level. These two video filter levels are for faster response than the High Quality Level as to increase the response speed over limited bandwidth condition. If your bandwidth allows or you need higher video quality instead of higher speed, just change the video filter from Low to Medium or even to High to increase the video display quality on viewer screen on the remote login client. To raise the Video Filter Level, please go to the Video Server Page in KLE web management Interface, and select the filter as either Medium or High Quality according to your requirements. Note that High Quality video filter gives high quality always on the expense of video response speed on the viewer screen.

(2) The transitional effect of Windows XP is enabled. The transition effects of menu will cause refreshing problems in Low/Medium Video Filter settings. Thus, if you are using a Low/Medium Quality Level of video filter, either try to raise the video filter level to High Quality (at the expense of response speed) or just turn off the transitional effects of Windows XP. To turn off the transitional effects of menu on Windows XP, please refer to Section 2.2 , Configure your Computers for Connections to KLE

Note that KLE local console is not affected at all by the Video Filter settings or by the transitional effects on Windows XP.

Q. The KLE booting time has become unduly longer over several minutes. What's wrong?

A. Please make sure that the external authentication, PPP server/client, time server as well as power control settings are correct. If you don't use all these features or the authentication/time servers are not available, just try to disable them to save booting time since if you don't have all these servers present, the KLE will try to look for them until timeout. That will waste KLE booting time considerably.

Q: Video response seems slower in limited bandwidth condition, are there ways to increase the response speed?

A: There are several ways to increase the response speed on the viewer screen:

(1) Under bandwidth limited condition, you should select a more economical encoding scheme such as Slow Internet or Fast Internet Encoding scheme instead of the LAN or No Compression encoding scheme from the viewer connection option menu. However, if the connection is made only within LAN with plenty connection bandwidth, LAN or No Compression encoding scheme should be (paradoxically) quicker than Internet scheme – since your client computer won't dissipate extra computing power for decoding the more-compressed Internet scheme.

(2) Use 8-bit color reduction (with only 256 colors instead of the 65K colors in 16-bit settings).

(3) You can enable Automatic Filter Adjustment (web management/Video Server page) for automatic video optimization according to different bandwidth condition.

(4) On the other hand, if you don't want to use Automatic Filter Adjustment, you could always select either Medium Quality/Low Quality level for more speed as your Video Filter setting (web management/ Video Server Page). You could also do something to increase the response speed: use a server desktop of small resolution (such as 800 x 600) and use a solid plain color background for server desktop.

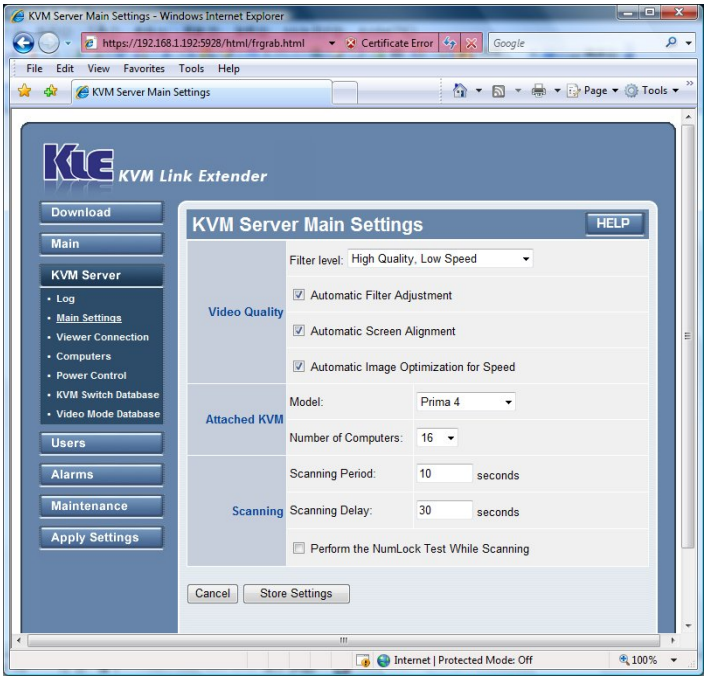
(5) Finally, you should check the networking environment. Try to find bottlenecks that can be improved or eliminated for more bandwidth throughput.

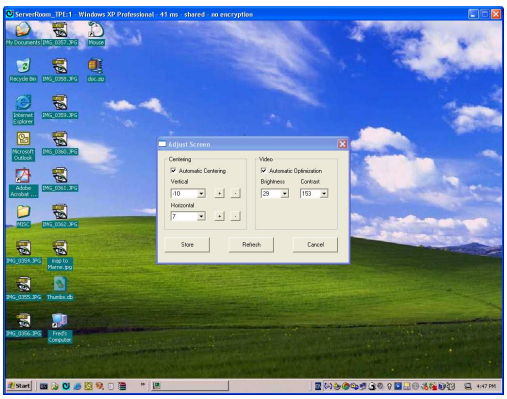
Q. When connection is first made, the display on the viewer screen seems not centered correctly and there is black margin on the edge of the viewer screen. How could I eliminate the black strip?

A. The black strip is the offset that will be seen when the display on viewer screen is not centered corrected. Probably you have not enabled automatic centering option on KLE, so please check the followings:

(1) Go to the Video Server page on KLE web management Interface to check whether the Automatic Screen Alignment option is enabled. If it is not yet enabled, please check the option, click Submit button and then go to Apply Settings page to click the Apply Settings button to restart KLE with new setting.

(2) When the viewer connection is made, select the Adjust Screen option on Viewer's Quick Menu, and the Adjust Screen dialog box appears. On it, check whether you have Automatic Centering enabled. If it is not yet enabled, please check this option to enable it. If it is already checked, please uncheck it and then wait for at least 15 seconds. Then check the option again to force the video server to align (center) the display in the viewer screen.





Q: I can log in and make successful browser connection with KLE. However, I cannot make a valid viewer connection or the KLE does not respond to my viewer connection request.

A: The KLE video server might not function properly. First, make sure your account have the SUPERADMIN privilege. If not, you should request one that has the SUPERADMIN privilege to do the troubleshooting job for you.
First, go to the *Apply Settings* page on the web management interface and then click the *Apply Settings* button to restart KLE. Then wait for at least 10 more seconds for it to start completely. Try to make the viewer connection again to see if it is back to normal.
Second, If the *Apply settings* button could not bring back the KLE video server to normal working condition, try to hit the *Emergency Reboot* button (could be found on the *Maintenance* page of the web management Interface) for a complete start from ground level. An *Emergency Reboot* is a clean reboot, and it takes longer time for KLE system and video server to load, thus you have to wait at least one minute for the system to be up and running.
Then try to make the viewer connection again to see if it is brought back to normal function again. A cold boot of KLE is always a last resort to bring the KLE back – just try to disconnect the power adapter form KLE and wait for sometime (30 seconds) before plugging in again for a cold start over.

Chapter 4
KLE Unit Management

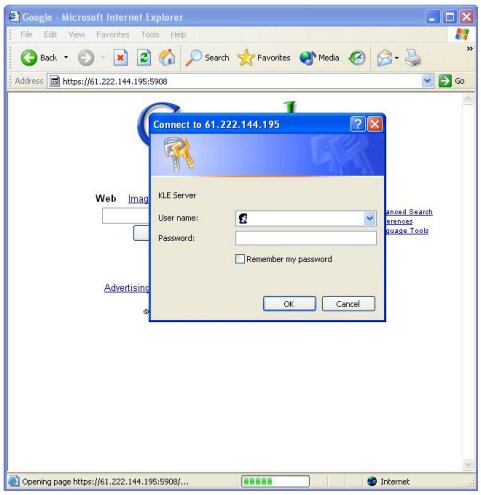
KLE's web management interface uses only password authentication to authenticate login user's identity. After user identity is authenticated (that is, if you have typed in the right user name with a right password in the login prompt…), an SSL-secured browser connection using 256-bit cipher strength is established.

4.1 Web-based Management Interface

Type in the correct IP address and port number:

```
https://<IP_address>:<port_number>

https://61.222.144.195:5908
```

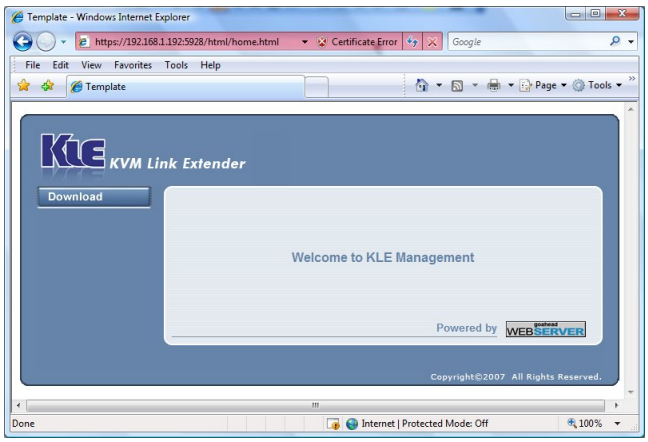


Remember that it is a secure SSL encrypted connection, so you should type "https" instead of the usual "http". Otherwise, the connection will not be established. The port number might vary according to its setting on the KLE server. By default, the browser connection uses port 5908. **Both user name and password are case-sensitive.**

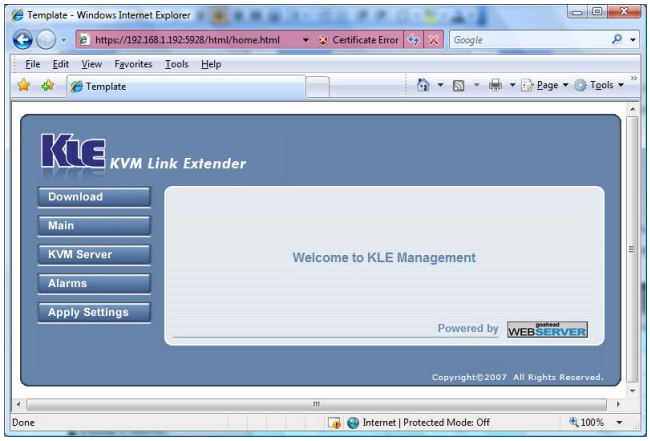
4.2 User Privileges – SUPERADMIN, ADMIN, USER

KLE offers three categories of user privileges for web management: SUPERADMIN, ADMIN and USER.

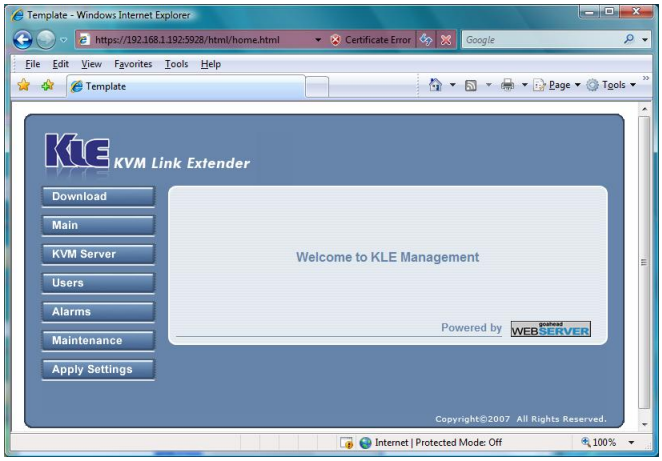
SUPERADMIN – Full access to web management features [and Power ON-OFF feature on viewer]
ADMIN - Partial access to web management features [and Power ON-OFF feature on viewer]
USER – Only minimal access to web management features (only the Download and the Logout pages)



Minimal Access (User



Partial access – ADMIN

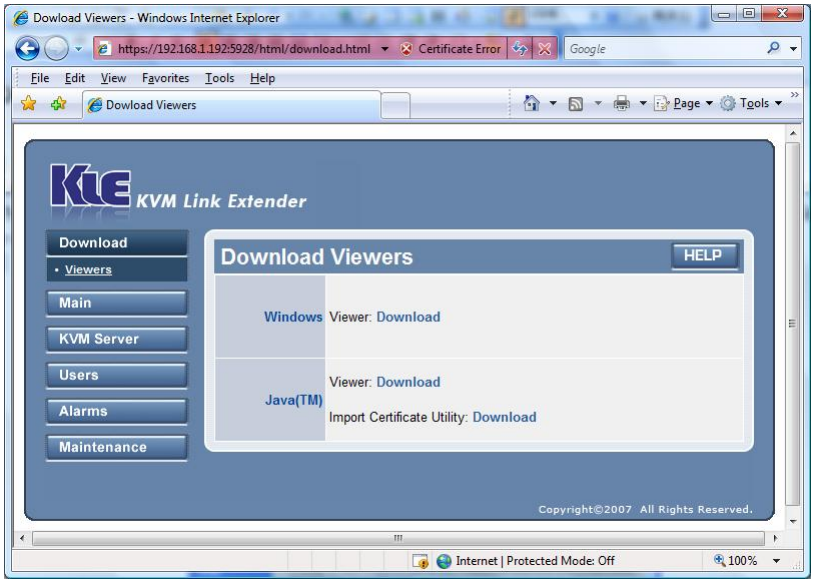


Full access – SUPERADMIN

KLE Browser Management Access Privilege			
Feature Page	**SUPERADMIN**	**ADMIN**	**USER**
Download	√	√	√
Main	√	√	×
KVM Servers	√	√	×
Users	√	×	×
Alarms	√	√	×
Maintenance	√	×	×
Apply Settings	√	√	×

4.3 Download/Viewers – Download Programs for Viewers

The download page allows you to download both Windows and Java (TM) Viewers.



KLE Viewer Download Page

Windows

The viewer for Windows can run on most of Windows platforms: 98/Me/NT/2000/2000 Server/XP/2003 Server/Vista. Click Download and follow the installation instructions.

Note: If you wish to use the secure full SSL connection (security level 3), get a set of certificates from your administrator. Install the certificates on your computer by running the ImportCertificate utility provided with this viewer. Refer to the Security page.

Java ™

The viewer for Java is truly cross-platform for all major Operating Systems including Windows, Linux, Mac OS, etc. However, before you can run the Java viewer on any computer, you must first install the Java Runtime Environment (JRE), which is freely available from Sun at http://www.java.com/. It is recommended to get JRE 5.0 or higher.

On Windows machines, a simple double mouse click should permit to start the viewer for Java. If the viewer does not start automatically, check the .JAR file association on your computer. It must be javaw.exe (and NOT javaws.exe). On other machines, download the KViewer.jar file into a folder and type:

```
java -jar KViewer.jar
```

Note: Some Browser will automatically change the file extension from .jar to .zip while you are downloading the file. If this is the case, please change the file extension back to .jar, so that you can run it properly.

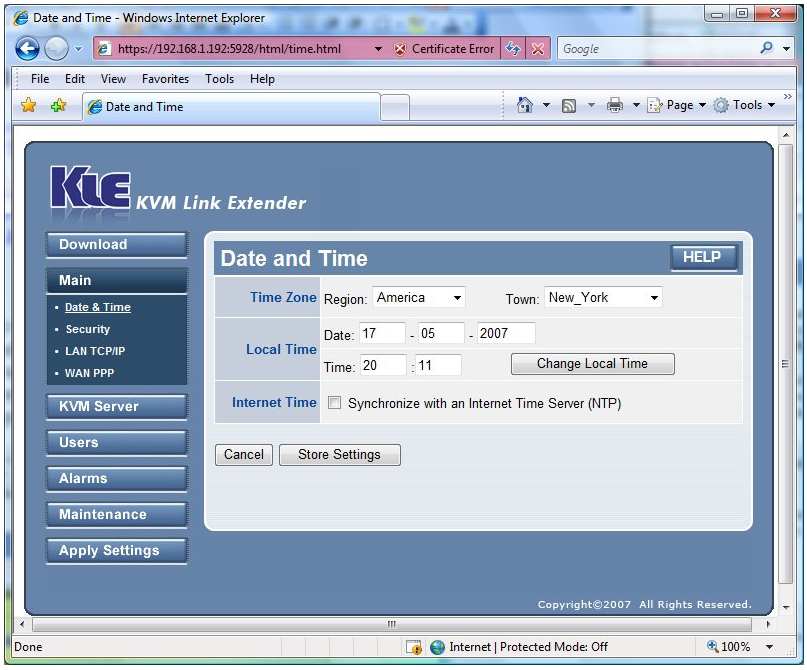
Note: If you wish to use the secure full SSL connection (security level 3) with the Java Viewer, get a set of certificates from your administrator, download the Import Certificate Utility Impcert.jar file into a folder and type: java -jar Impcert.jar. Refer to the Security page.

4.4 Main/Date & Time – Date, Time, Global Time Zone Support and NTP server Synchronization

The Date and Time page allows you to configure time-related settings of your KLE, including Time Zone settings, Local Time and Internet Time.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart* Servers!



Time Zone: Select the Time Zone/Region and City/Town from the available list as seen in the drop down combo boxes.

Local Time: Enter the correct date (dd-mm-yyyy) and time (hh:mm) here and click Change Local Time button to set current system time on KLE. Note that if you check the option to automatically synchronize with an Internet Time Server (NTP), the time setting will be periodically synchronized to the time of NTP server specified on each restart of the KLE and every hour.

Internet Time: This option, Synchronize with an Internet Time Server (NTP), is for the automatic time synchronization of KLE with an available timeserver on the Internet. You can check the option and then specify the timeservers you prefer. The KLE will try to synchronize with the timer servers every time it starts or restarts and will continue to synchronize every hour thereafter.

> **Note:** if you choose this option the original Current Date and Time settings you manually entered will be refreshed with the time provided by the Internet timeserver.

NTP Server1: is the server, with which the KLE will first try to synchronize, and the NTP Server2 is the backup timeserver, with which the KLE will synchronize when the first timeserver is not available. Enter the domain name of the timeserver.

> **Note:** There are many Internet timeservers available. You can search in the Internet for ones that are nearer to the location where you install the KLE. You should choose your Internet timeservers based on the principle that a timeserver nearer to you will reduce time latency in synchronization.

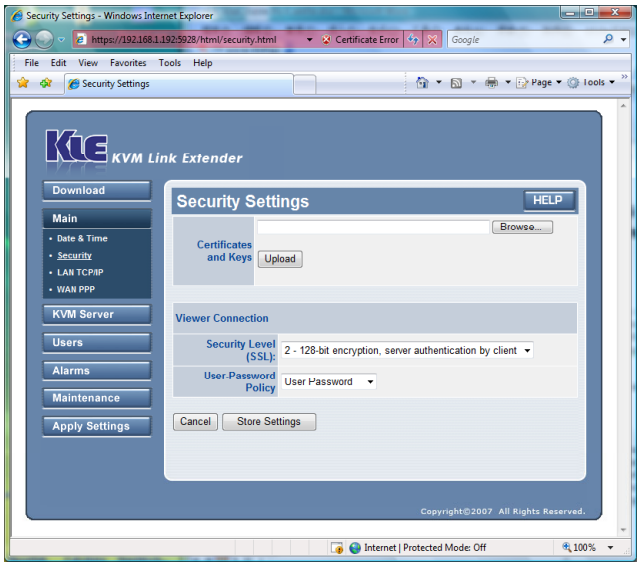
4.5 MAIN/Security – Certificates, Viewer Encryption and Password Policies

The Security page enables you to configure and implement security-related settings of your KLE, such as uploading your certificates for the KLE server side, selecting the security level of the viewer connections, and the password policy for the viewer and browser connections.

Security settings should be taken very seriously. If KLE security settings are set to *No Password,* no SSL, and no PKI authentication (Viewer connection security - Level 1), almost anyone can establish a remote connection. With these settings, you probably will not "survive" longer than 15mn on the Internet without someone is trying to access your computers.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



4.5.1 Certificates and Keys

Certificates are only needed if you intend to implement full PKI authentication for the viewer connections. If an SSL-encrypted session is already enough for your security requirements, you can just ignore this aspect of PKI authentication.
Where can you get the certificates? There is a default set of certificates in your support CD ROM. You can use them to practice the certificates uploads. In real world scenario, you can either generate the certificates by yourself, since there are some freeware or shareware such as XCA for this purpose. You can also buy certificates from companies that provide authentication service.
The valid file names and formats of the certificates and Keys to be uploaded to the KLE should be exactly as below:

- root.crt
- server.crt.
- serverkey.pem
- ldapcert.crt
- ldapkey.pem

4.5.2 Security Level of Viewer Connections

The browser connections to the web management are **always** using SSL connections. The viewer connections can use different levels of security.

Security Level (SSL): The KLE offers three levels of security for viewer connections. On the drop-down combo box, you can just choose either one of the three viewer security levels as appropriate to your real demands on viewer connection security:

Level 1 uses No SSL data encryption and No authentication. This is the most straightforward setting that opens most convenience if there are no security concerns at all. Anyone who have a viewer and an Internet connection can easily connect to KLE as long as the user passes the password policy requests.

Level 2 uses SSL encryption for viewer connection, but only requires server authentication by viewer client. Remote users are not require to install any certificates on their client computers. However, the viewer connection is encrypted with 256-bit SSL technology to ensure that all data contents transmitted via the viewer connection are protected, including keyboard, mouse and video signals.

Level 3 uses 256-bit encryption and a bi-directional PKI authentication between KLE server and viewer client. With this level of security, all remote users who want to make viewer connections must install a proper client certificate on their computer. This client certificate must come from the same CA that issued the root.crt certificate of KLE.

KVM Server Password: This item will only appear if you choose to implement Level 3 security. Here you should enter the password that has been used to protect the server private key serverkey.pem. If you use the standard set of certificates provided by default on the Support CD ROM disc, the server password is **serverpwd**. However, if you use your own set of certificates (as you should do for a real secure installation), you must set the correct server certificate password you got from the Certificate Authority that issued those certificates.
First, you should get a set of certificates from your administrator. If your certificates files have different names, change them to the valid names before uploading.
To upload the certificates, click the *Browse* button to go to the location where your certificates reside. Select a certificate file and then click *Upload* to upload your certificates, one at a time, to the KLE. After the uploading is completed, you should see the prompt page for reboot. However you don't have to reboot before you have uploaded all the necessary certificates. Just reboot once after you have uploaded all the necessary certificates: **root.crt ; server.crt ; serverkey.pem**

You must upload two extra certificates if you need to SSL-encrypt the LDAP connection for user remote authentication: **ldapcert.crt; ldapkey.pem**

4.5.3 User Password

User-Password Policy: The KLE offers three types of password policies for selection, you can select here your password policy for viewer connections:

- **No Password:** the viewer will not prompt you for any user password - the door is open unless you are using security level 3.
- **Global Password:** the viewer will prompt you for a global user password, which is used by all users - a sort of building door code.
- **User Password:** the viewer will prompt you for your user-specific password - a sort of apartment door code.

Note: The viewer can also prompt you for the client certificate password if you are using the security level 3.

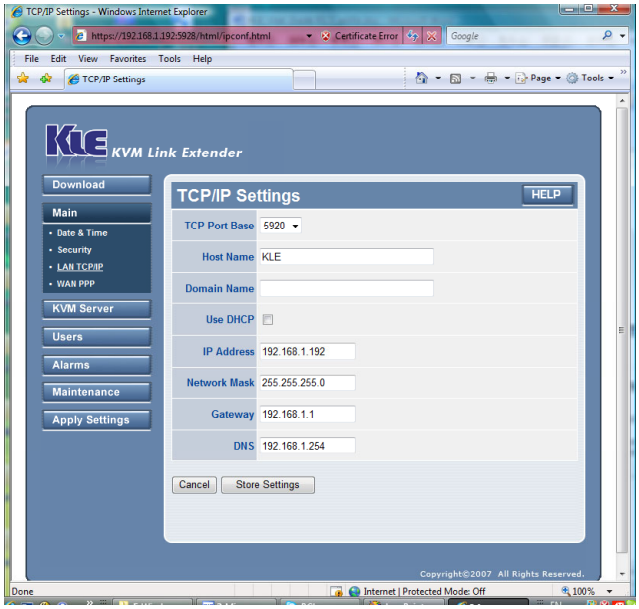
Global User-Password: This item only appears if you select *Global Password* as password policy. Enter the common password used by all users here.

4.6 MAIN/TCP/IP Settings – Port and IP settings

The LAN TCP/IP page is where you can set up the TCP/IP settings of your KLE. Here you can specify the IP address, net mask, gateway address, DNS address and access port base for viewer and for browser (port base +8), or whether you want to use DHCP.
However, before you go on with the various settings on this page, you might need to check first with your network administrator for proper settings. If you do not configure those TCP/IP settings properly, you will not be able to make valid connections to the KLE.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



TCP Port Base: You can freely specify the port base for viewer connection with the KLE server. You can choose any available port base, starting form the lowest alternative of port 5900 with an increment of 10 right up to port 6090. The port base you choose is exactly the port number that KLE uses for viewer connection. "port base + 8" is the exact port number you will use for secure http connection for the browser. After you have made the port base modification, remember to hit the Store Settings button, and then hit the Apply Setting/Restart Servers to validate your changes.

Host Name: The host name is the name that the KLE will assume on your Local Area Network.

Domain Name: Specify here the domain name for your KLE as it appears on your LAN. (Leave it empty if you don't know).

Use DHCP: This option allows the KLE to get all TCP/IP settings automatically from a DHCP server.

IP Address: Enter a fixed IP address (in dotted decimal format such as 192.168.1.200) that will be used by the KLE in your LAN.

Network Mask: Enter a net mask value (in dotted decimal format such as 255.255.255.0) that will be used by KLE in your LAN.

Gateway: Enter the fixed IP address (in dotted decimal format such as 192.168.1.254) of the gateway (i.e. router) to access the Internet.

DNS: Enter the IP address (in dotted decimal format such as 80.10.246.30) of the DNS server that will be used by KLE for domain name resolution. Ask your network administrator if you don't know.

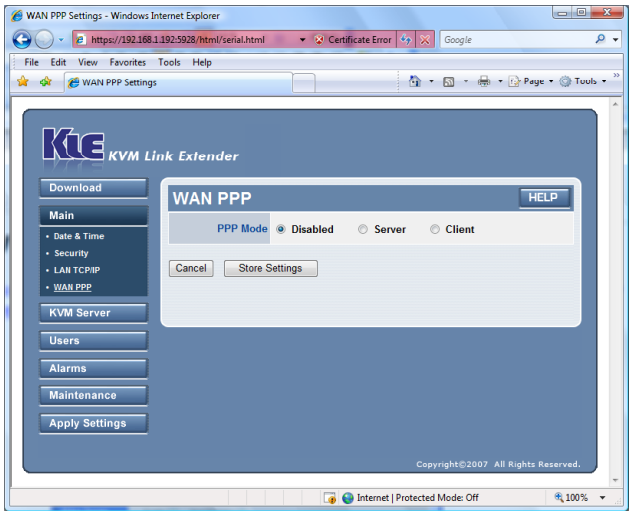
Note: You must enter a valid DNS server IP address to allow the email alert of KLE to be effective.

4.7 MAIN/WAN PPP

The WAN PPP page is where you can set up the PPP server/client mode of your KLE. Here you can enable either the PPP server mode, or the PPP client mode, or you can disable the PPP modes altogether.
The KLE can serves either as a PPP server for the remote computers to dial-in for connection, or as a PPP client to dial in a PPP server to connect to a network or the Internet. The PPP connection can serve as a backup connection mode when direct network connection is not available or just broken down. The KLE's high-speed serial interface can offer excellent bandwidth to PPP connections either when the KLE is connected as PPP server or PPP client.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



4.7.1 PPP Modes

There are three PPP options for selection:

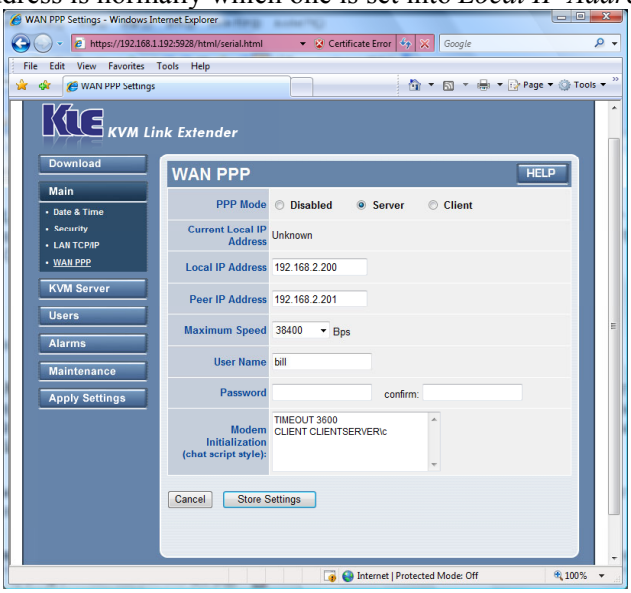
- PPP Disabled: by default.
- PPP Server mode: for connection request from a peer computer.
- PPP Client mode: for dial-in connection to a PPP server (your ISP or an Enterprise PPP Server)

The PPP Server mode allows users to connect to your servers without the Internet understructure. It can be used as a backup access in case of Internet failure or an ultra-secure access by the use of private lines and modems.
The PPP Client mode can be used when there is no LAN or router available for a direct Internet access by using a modem.

> **Note:** The PPP connection can work simultaneously with the LAN connection.
>
> **Note:** The PPP connection uses the same serial interface as the Power management. These two features are mutually exclusive. By enabling the PPP you automatically disable the power management and vice versa.
> If you have a LAN connection, normally you don't have to choose the PPP connection as your connection mode. However, if no LAN connection is available or if you want to use , you could choose to enable either the PPP server mode or the PPP client mode according to the real connection scenarios.

4.7.2 PPP Server Settings

Current Local IP Address: This is where you can check up the IP address of the KLE when a PPP connection is established. However, if the PPP connection is not yet established, the IP address will be shown as *Unknown*. This address is normally which one is set into *Local IP Address*.



Note: This IP address must be distinct from the one that is used by the KLE on the LAN.

Local IP Address: Enter here the IP address (default = 192.168.2.200) to be used by the KLE in the PPP connection. This IP address will be used only in PPP connection by KLE alone, and should be distinct from the IP address (default = 192.168.1.200) that is specified in the *LAN TCP/IP* page and used for connection via direct local area network.

Peer IP Address: Enter the IP address (default= 192.168.2.201) that will be assigned by KLE to the peer client at connection time.

Maximum Speed: Specify the modem connection speed. The KLE supports a high-speed serial connection up to 1 Mbps (Megabits per second).

Note: the modem connection speed is NOT the PPP connection speed, which depends on the modem technology. For example, even if the modem connection speed is 115 200 bps, a 56K modem will provide only a 56 000 bps PPP connection.

User Name: Specify the user name that must be used for the PPP connection login by the peer computer on the other side of the phone line/serial connection.

Password: Specify the password that must be used by the peer computer, then type in the same password in the next entry field to confirm the password.

Note: KLE can support only one User Name / Password and one PPP connection at a time.

Modem Initialization (chat script): The modem initialization script is a chat script that will initialize the modem to be ready for connection. The standard script provided by default permits to connect a Windows client to KLE in server mode over a direct serial cable (Null Modem).

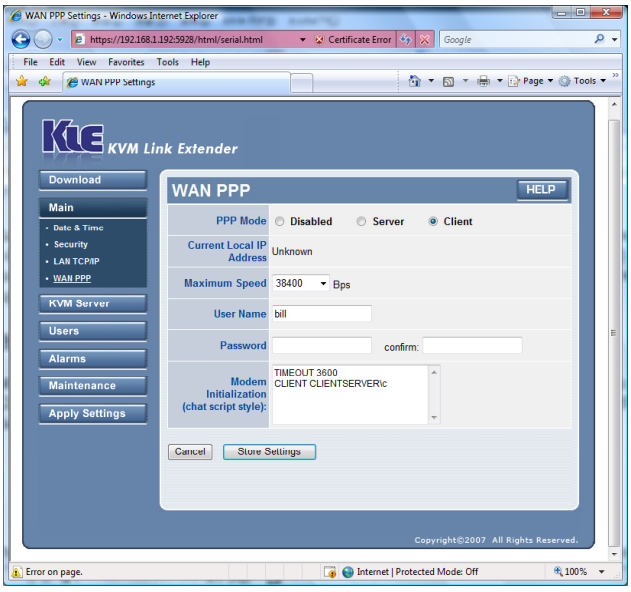
```
TIMEOUT 3600
CLIENT CLIENTSERVER\c
```

In other words: wait for "CLIENT" one hour, and respond CLIENTSERVER without carriage return.

Note: Refer to *Power Management* page for more details about the chat program. Refer also to your modem documentation. We also strongly recommend you refer to the standard man pages of pppd and chat programs on Linux. In server mode, the modem should be set to await and automatically connect when receiving remote calls.

4.7.3 PPP Client Settings

Current Local IP Address: This is where you can check up the IP address assigned to KLE by the PPP server at connection time. For example: 62.147.111.39. However, if the PPP connection is not yet established, the IP address will be shown as *Unknown*.



Note: This IP address is used by the KLE either as a PPP client, and thus is distinct from the one that is used by the KLE on the LAN.

Maximum Speed: Specify the modem connection speed. The KLE supports a high-speed serial connection up to 1Mbps (Megabits per second).

Note: the modem connection speed is NOT the PPP connection speed, which depends on the modem technology. For example, even if the modem connection speed is 115 200 bps, a 56K modem will provide only a 56 000 bps PPP connection.

User Name: Specify the user name that will be used by the KLE to connect to the PPP server.

Password: Specify the password that will be used by the KLE to connect to the PPP server.

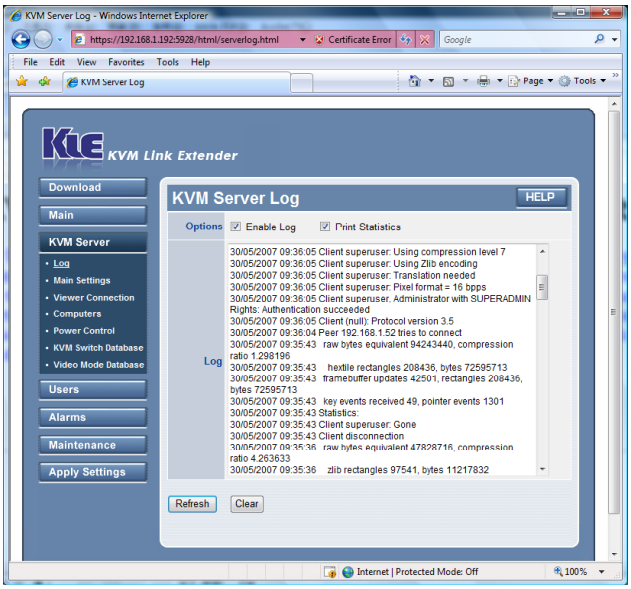
Note: The user Name and Password are normally provided by the ISP at subscription time.

Modem Initialization (chat script): The modem initialization script is a chat script that will initialize the modem to be ready for connection. The standard script provided here by default cannot work for a client connection. Replace it with your own initialization script depending on your modem.

Note: Refer to *Power Management* page for more details about the chat program. Refer also to your modem documentation. We also strongly recommend you refer to the standard man pages of pppd and chat programs on Linux. In client mode, the modem should be set to dial automatically at start time.

4.8 KVM Server/Log

This Server Log Page keeps a detailed record of events, beginning from each restart, of each user login, port switching actions, and video modes therewith. It also records each login attempt and the IP address from which the login attempt has originated, even if the attempt is not successful. It will show certain technical details such as the compression ratio, encoding scheme and bytes transmitted in each successful viewer session. This is the place where you should go check first if you want to know the usage/health conditions of your KLE.



Enable Log: check this option to enable the logging of KLE server events. If you choose not to enable this option, no logging will be done.

Print Statistics: If you need to know more about the KLE server statistics such as the compression ratio, bytes transmitted, rectangles drawn, frame buffer updates, and key events received, etc., you can check this option so that you can have quantified data for the profile of each session. To record the statistics of the video server and port switching activity by KLE remote users, you should check this option to print statistics to the server log file.
Each log entry is preceded by date code, time stamp and then the description of the specific log event. You can check here for the IP address that is assumed by the login user when they made the login attempt, and you can check the statistics of each session as a useful reference for the quantified data of each viewer connection. Note that the log file is of a definite size; older log entries will be erased when the log file has reached its maximum size while newer logging events keep coming in.
Click the *Refresh* button to refresh the screen output of the log file. Since newer server events may have happened and being logged to the database after your previous access of this server log page, you need to click the *Refresh* button to reload the log messages.
Click the *Clear* button to erase the log file contents in the database.

Note: The server log is erased each time you perform a complete reboot remotely by hitting the *Reboot* button in the Maintenance/Reboot page or when KLE suffers a power loss.

4.9 KVM Server/Main Setting

This page allows you to set up the KVM server operation: video quality and optimization, KVM switch model, auto scanning function.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!

4.9.1 Video Quality

Filter Level: Specify here the Video Filter Level for the KLE video server. Based on the bandwidth availability, you can select one of the three modes of video filter levels:
High Quality, Low Video
Medium Quality, Medium Speed
Low Quality, High Speed
Each of the three video filter levels is adapted to different combination of video quality and bandwidth requirements. Users can select their preference according to their actual video quality preference and network bandwidth availability. However, there's always a trade off between video-quality and response-speed when under limited network bandwidth.

High Quality, Low Speed (Light Filter): This level is recommended for high bandwidth networks such as LAN or broadband Internet. It requires more bandwidth than the other two filter levels and video refresh speed is slower (however, only noticeable when bandwidth is very limited). This filter provides the best image quality.

Medium Quality, Medium Speed (Medium Filter): This level is recommended for Internet connections. It requires more bandwidth than the Low Quality High Speed, option. This is most often the best speed / bandwidth compromise.

Low Quality, High Speed (Strong Filter): This level is recommended for very limited bandwidth conditions, such as a dial-up modem line to the Internet. With this setting, the viewer screen is updated only on big video changes. Most of time there will be no transmission at all.

Automatic Filter Adjustment: When this option is checked, KLE can tune the video filter automatically for optimized performance according to the current bandwidth availability.

Automatic Screen Alignment: When this option is checked, KLE tries to center the view screen automatically to eliminate the offsets sometimes seen in the viewer screen as black gaps.

Automatic Image Optimization for Speed: When this option is checked, KLE tries to optimize the video settings (phase, light and contrast) to produce images of better quality with higher compression.

4.9.2 Attached KVM

Model: If you ever use a KVM Switch behind the KLE for connection with multiple computers, you should then select the model of the KVM Switch. If the KVM switch model does not appear in the list, you can always add it or even add more KVM switch models to augment the list, so that your computer icons (as you see on the Select Computer box) can support the port switching hotkeys of that specific KVM Switch upon clicking. For more information on how to add a KVM switch model to the KVM switch database, please refer to the *KVM Switch Database* page. For more information on how to name a computer as it appears on the computer icon of the Select Computer box, please refer to the *Computers* page.

Number of Computers: Specify a maximum allowable number for total connected PCs for the KVM Switch attached behind KLE. You can specify a maximum of 256 computers, as you might have a configuration of several cascadable KVM Switch units behind KLE.

4.9.3 Scanning

Scanning Period: The scanning period is the default scanning duration for each connected PC, if no KVM (Keyboard - Video - Mouse) event happens to interrupt the scanning. If there is a KVM event such as keyboard/mouse movement or video resolution change, the scanning will be temporarily held until it reaches the timeout of the scanning delay, and then go scanning to the next. Here you can specify the scanning period in seconds.

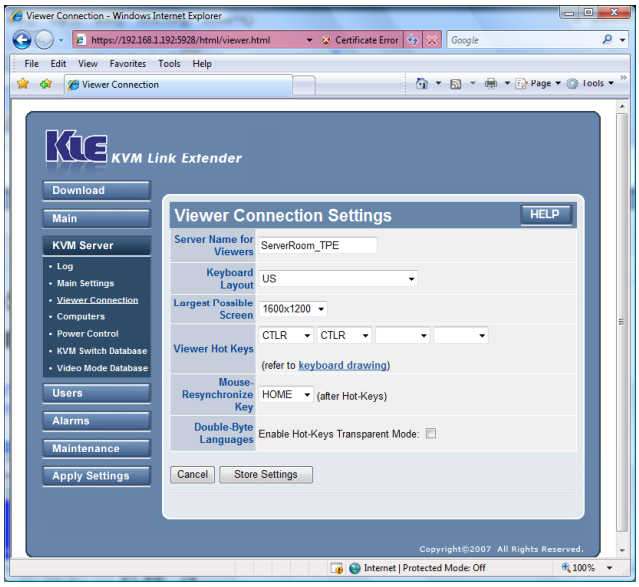
Scanning Delay: The scanning delay is the time that KLE will wait after it last perceives a KVM (Keyboard - Video - Mouse) event before it switches to the next connected PC.

Performing the NumLock Test while scanning: The NumLock test is a way to detect whether a computer is still responding to keyboard action. If you check this option, KLE will send a NumLock signal to the PC while scanning. If the PC returns a response, then he NumLock LED will be lit. The NumLock test can serve as a test to see if the connected PC is still responsive to keyboard event. The NumLock signal will serve as a "wake up" signal if the PC is in sleep mode. If the NumLock test has failed, it most likely indicates that your computer is in trouble. Check this option if you want to use auto scanning to monitor whether each of your computers has stayed alive or not.
You can also specify which computer will be included and which computer will not be included within the auto scanning process. For more information on how to add or remove computers from the auto-scanning list, please refer to the *Computers* page.
Also, if combined with the Alarm options, auto scanning can detect critical server problems such as No Video, Blue Screen, NumLock Test failure on first timing basis, and send either an alert email or SNMP message, or power cycling commands to a Serial Power Control device to power cycle the server in problem. For more information on how to configure the alarm features of KLE, please refer to the *Alarms* pages.

4.10 KVM Server/Viewer Connection – Video Server Name and Keyboard Type Settings

This page allows you to configure settings proper to the viewer, including the name as it appears on the title bar of the viewer window. The keyboard layout that KLE will assume must be consistent with the one you use on the client side. Set the biggest resolution support, the mouse re-sync hotkey sequence, and the *Hot-Keys Transparent Mode* - very convenient and useful feature for anyone who uses double-byte language such as Chinese, Japanese or Korean (the CJK languages) and some other languages.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings. No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



Server name for Viewers: Enter here the server name you chose for the Video Server on KLE and it will appear on the title bar of your KLE Viewer window.

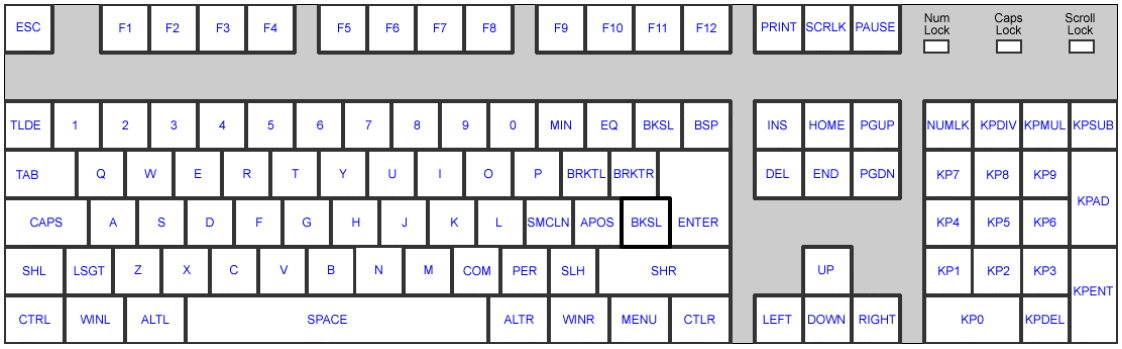
Keyboard Layout: Choose the keyboard layout for the KLE according to the real keyboard you are using on the remote login client. Choosing the correct keyboard layout for your keyboard is very important since some key codes are represented by different key locations in different keyboard layout. A correct keyboard layout setting ensures that you will have a matching key code output on the server side as what you have input on the physical keyboard from the client computer side. The default keyboard layout is the *US* keyboard (*US*). The KLE supports more than 60 types of keyboards all over the world.

Largest Possible Screen: The KLE supports a maximum resolution up to 1600 x 1200 pixel dimension. Normally, if you select the biggest resolution support of 1600 x 1200, it will be most accommodating to all display resolution requirements. However, you can still select a smaller workable resolution for your display device. If you choose a smaller resolution, you have to be aware that any screen larger than what you specify here will not be shown on the viewer. The KLE supports resolutions as follows:

- 640 x 400
- 640 x 480
- 800 x 600
- 1024 x 768
- 1152 x 864
- 1280 x 1024
- 1600 x 1200

Refer to the *Video Mode Database* page for more detailed information about the refresh rate support.

Hot Keys: KLE can detect a special sequence of keystrokes when you type on your remote keyboard. This special sequence is used to ask KLE to resynchronize the local and the remote mouse cursors in a fast and convenient way. For example, it is faster to type CTLR–CTLR–Home on the keyboard than to use the mouse and select a command into a menu. For compatibility with higher devices, this command is divided in two parts called *Viewer Hot Keys* and *Mouse Resynchronization Key*.
Please be aware that the *Viewer Hot Keys* are transmitted to the KVM or server attached to the KLE. On the contrary, the *Mouse Resynchronization Key* is eaten by the KLE. Thus, because the *Viewer Hot Keys* are transmitted, they must be as harmless as possible. *Viewer Hot Keys* such as NumLock-NumLock, Scrlk-Scrlk or Ctrl-Ctrl can work because they produce generally no effect. On the contrary, the *Mouse Resynchronization Key* can be anything since it is not transmitted by TKIP-101.
The *Hot Keys* can be configured to fit your needs. To find out the key positions on a standard keyboard, please refer to the Keyboard Drawing.



Note 1: The *Viewer Hot Keys* are transmitted to the KVM attached. Thus, they must be chosen so that they don't interfere with the KVM hot keys.

Note 2: If you are running the Java viewer on Mac OS, you might find that the default mouse resynchronization sequence – CTLR-CTLR-Home - does not work. That is because the Right Control key on Mac keyboard sends out a different key code as the PC keyboard. If that is the case, you might consider configuring your *Hot Keys* as for example, CTLL-CTLL and S.

Viewer Hot Keys: Enter here your preferred keystroke sequence that will serve as Viewer Hot Keys. By default, this is **CTLR–CTLR,** in other words, two consecutive keystrokes of the **Right** Ctrl key (CTLR). **Please note that this is NOT the Left Control key (CTLL).**

Mouse Resynchronize Key: This is the only command supported by TKIP-101. It permits to synchronize the local and the remote mouse cursors. By default, this is the **HOME** key. Thus, by default you have to hit **CTLR–CTLR–HOME** to synchronize the remote and the local mouse cursors.

Double-Byte Languages: This feature makes KLE compatible with double-byte languages such as Chinese, Japanese or Korean. When using the viewer, if the remote computer and/ or your local computer is running a double-byte system, just type Alt and then Shift or Ctrl and then Shift **sequentially instead of simultaneously** to produce the same effects as usually.

Enable Hot-Keys Transparent Mode: Check this option if you are using **double-byte language** inputs on the local and/or the remote computer to facilitate switching between single-byte and double-byte inputs. Leave this option disabled if you don’t use any double-byte language.

4.11 KVM Server/Computers – Port and IP settings

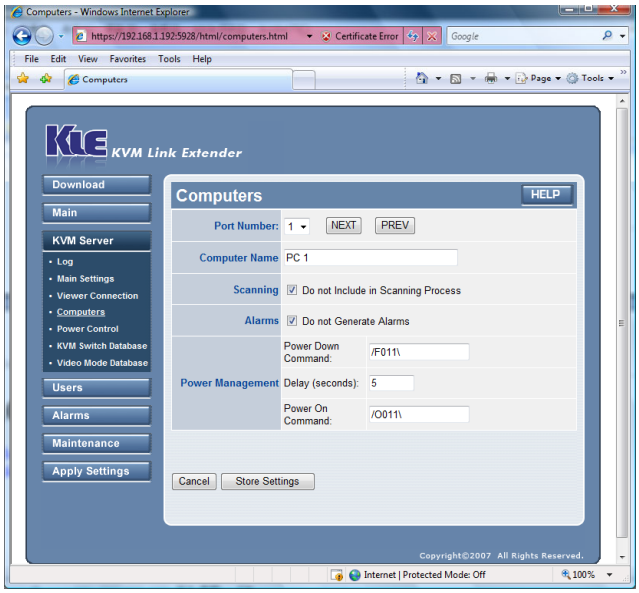
This page permits to provide KLE with information about all KVM-attached computers. This information is used by KLE to do some actions automatically in order to simplify your job:

- Work with computer names instead of KVM port numbers,
- Generate automatically the KVM switch hot keys to select computers. This allows you to select a computer with a simple mouse click or by using the computer name.
- Generate automatically (or on request) the power down and power on cycling if a power control unit is connected.
- Exclude some computers from the auto scanning process.
- Not generate alarms for some computers.

Note: You can also work without supplying any computer information. In this case, just keep the values by default. You will have to remember on which KVM port your computers are attached, and generate the specific KVM hot keys by hand. Note that most of low-end IP-KVM-extenders work this way.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Serve*rs to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



The various settings on this page are KVM port-specific because a computer is first identified by the KVM port to which it is attached.
Select the target port on which your subsequent settings on this page are directed. You can use the drop-down combo box as well as use the *Previous* and the *Next* button to navigate to a specific port.
Computer Name: Enter a character string of 32 characters maximum to identify the computer attached to the selected port.

Note: The computer names you specify here for each port will appear in the Windows and Java viewers.

Scanning: If you do not want this computer be included in the auto-scanning, check *Do not include in scanning process*. Thus, you can put a specific computer out of your radar screen if it is of no monitoring value.

Alarms: If you do not want the scanning process to generate alarm or SNMP messages for this specific computer, check *Do not generate alarm* to exclude it.
If you require power control for your connected computers, you can connect a serial power control (SPC) device to the serial port on the back side of the KLE, and then enable the power control feature on the KLE. Hence, remote users can then perform power on/off and power cycling either via the viewer interface, or by pre-defined alarm-triggered action. The KLE can support most of standard serial power control device via its serial port (RJ12) on back panel (Don't mix it up with the serial console port on the front panel). To enable the KLE power control feature, please refer to the Power Control page.

Important Note: when using a power control device, please note that some newer computers will require some BIOS option adjustment to restart when power is coming back. Otherwise, they will not restart without a push of the computer power button. Usually, you should enable the *Power Loss Restart* option on your computer BIOS (or similar option depending on the BIOS vendor), so that your computer can boot up when the power control device is feeding power again.

Power Down Command: Specify here the command that must be sent to the power control unit to power down the computer. Refer to your power control unit documentation.

Note: To remotely power-down this computer from the Windows or the Java Viewers, switch to this computer and then click *Power off* in the Viewer menu. The command specified here will be sent automatically by KLE to the power control unit.

Delay: Here you should specify the delay time between the sending of power-down and power-on commands to complete a power cycling. A power cycling is processed only if you have selected *Restart Computer* into the *Alarm page.* By default, this delay is 5 seconds.

Power On Command: Specify here the command that must be sent to the power control unit to power on the computer. Refer your the power control unit documentation.

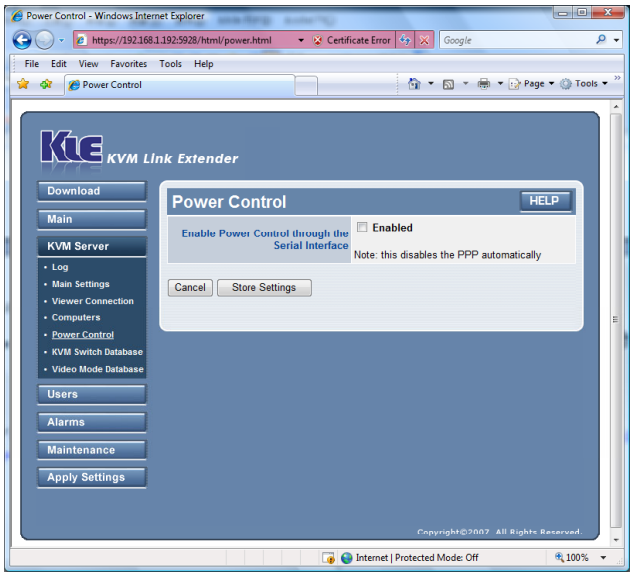
Note: To remotely power-on this computer from the Windows or the Java Viewers, switch to this computer and then click *Power off* in the Viewer menu. The command specified here will be sent automatically by KLE to the power control unit.

4.12 KVM Server/Power Control – Enable the power control

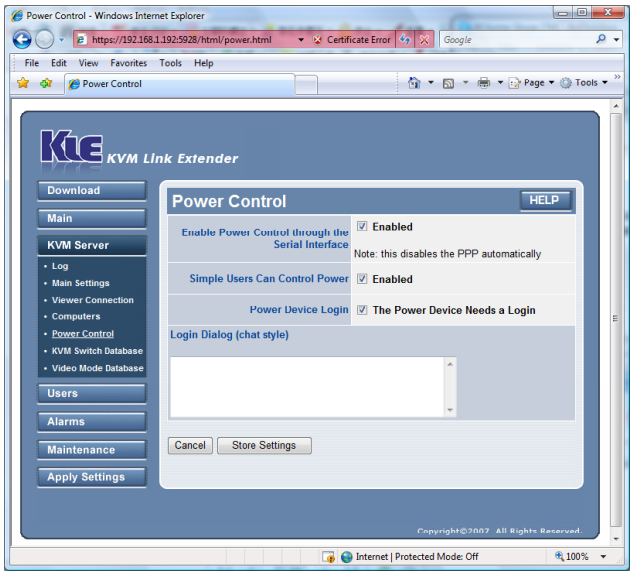
The Power Control page allows you to enable or disable the power control feature via the serial port on the back panel of your KLE. You can also specify the login script of your power control device, if it requires a login script.

After you have made all modifications, click *Store Setting*s to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



Enable Power Control through the Serial Interface: Check the *Enabled* option to activate the remote power control support feature of the back panel serial port of the KLE. Once this option is checked, a subsequent *Power Device Login* option will appear for you to decide whether to enter the login script.



Simple Users Can Control Power: Check this box if you want that simple users be able to power on and power off the computers.

Power Device Login: Depending on the Serial Power control device you used behind KLE, sometimes you will need a login script to login or initialize your power control device. If that is the case, just check the *Power Device Needs a Login* option, and a Login Dialog field will appear for you to enter your login script.

Login Dialog (chat style): This editable field is where you should enter the login script for your power control device, if it is required by your power control device. You should refer to the user guide of your power control device for correct information. A script consists of one or more "expect-send" pairs of strings, separated by spaces as in the following example:

```
login: myid
password: mypass
```

This script indicates that the KLE should expect the string "login:". Once it received "login:" , KLE sends the string "myid" and then expects "password:". When it receives the prompt for the password, it sends the password "mypass". A carriage return is normally sent following the reply strings. It is not expected in the expect strings unless it is specifically requested by using the \r character sequence.
If the script must start by sending something instead of waiting for a string, use the null sequence " (two quotes with no space in between) as expect string:

```
'' restart
login: myid
password: mypass
```

In other words send "restart", expect "login:", send "myid", expect "password", send "mypass".

The expected sequence should contain only what is needed to identify the string. For example, to help correct for characters that may be corrupted during the initial sequence, look for the string "ogin:" rather than "login:". It is possible that the leading "l" character may be received in error and you may never find the string even though it was sent by the power device. For this reason, the script should look for "ogin:" rather than "login:" and "ssword:" rather than "password:" like this:

```
ogin: myid
ssword: mypass
```

In other words, expect "ogin:", send "myid", expect "ssword:", send "mypass".

A comment is a line which starts with the # (hash) character in column 1. Such comment lines are just ignored. If a '#' character is to be expected as the first character of the expect sequence, you should quote the expect string. If you want to wait for a prompt that starts with a # (hash) character, you would have to write something like this:

```
# Now wait for the prompt and send "logout"
'# ' logout
```

ESCAPE SEQUENCES

The expect and reply strings may contain escape sequences. All of the sequences are legal in the reply string. Many are legal in the expect string. Those which are not valid in the expect sequence are so indicated.
`''` Expects or sends a null string. If you send a null string then it will still send the return character. This sequence may either be a pair of apostrophe or quote characters.
`\b` represents a backspace character.
`\c` Suppresses the newline at the end of the reply string. This is the only method to send a string without a trailing return character. It must be at the end of the send string. For example, the sequence hello\c will simply send the characters h, e, l, l, o. (not valid in expect.)
`\d` Delay for one second. (not valid in expect.)
`\n` Send a newline or linefeed character.
`\N` Send a null character. The same sequence may be represented by \0. (not valid in expect.)

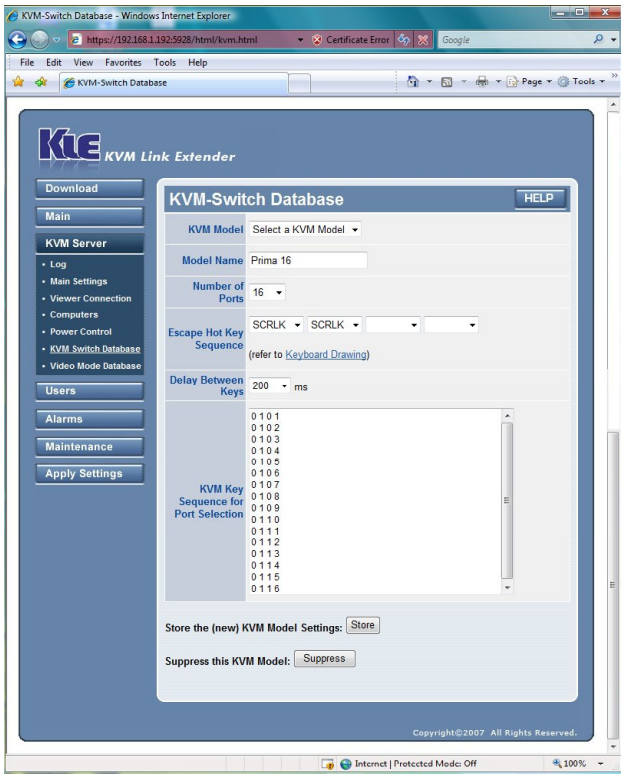
\p Pause for a fraction of a second. The delay is 1/10th of a second. (not valid in expect.)
\r Send or expect a carriage return.
\s Represents a space character in the string. This may be used when it is not desirable to quote the strings which contains spaces. The sequence 'HI TIM' and HI\sTIM are the same.
\t Send or expect a tab character.
\\ Send or expect a backslash character.
Refer to the Linux chat program man page (man 8 chat) to get more details.

4.13 KVM Server/KVM Switch Database – Keeping and adding your KVM database

This page allows you to select or to create a KVM switch model to be used behind the KLE.

After you have made all modifications, click Store Settings to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



KVM Model: Here, in the drop down combo box, you can take a brief look of all the currently supported KVM models built into this database. Normally, you don't have to care about this KVM database, unless you need to modify the port switching sequence of an available KVM switch model, or, you want to delete an entry, or, you need to create a new entry into the existing KVM Switch list.

Model Name: *Model Name* shows the model name of the KVM switch you have selected from the drop down box above, and the subsequent parameters as shown in below are all pertaining to that KVM switch models, as regarding port number, Escape hotkey, key delay, and port-switching sequence, etc. If you want to add a new KVM switch entry into the existing list, enter the name of the new KVM switch and go on subsequent settings for that specific KVM switch.

Number of Ports: This is where you can specify the maximum port capacity of the selected KVM Switch model. Note that that some models can be daisy-chained together to expand the total port capacity. If you intend to add a KVM switch model to the database and use it as in daisy-chained configuration with other KVM switches, you should here specify its maximum port capacity as expandable in this configuration. KLE allows a maximum setting of up to 256 ports.

Escape Hotkey Sequence: To select the active port, the conventional KVM switches use to provide buttons and/or hotkeys and/or OSD menu. KLE cannot drive those low-end KVM switches that cannot switch with something else than buttons (usually two-port KVM switches). On the contrary, KLE can drive all the KVM

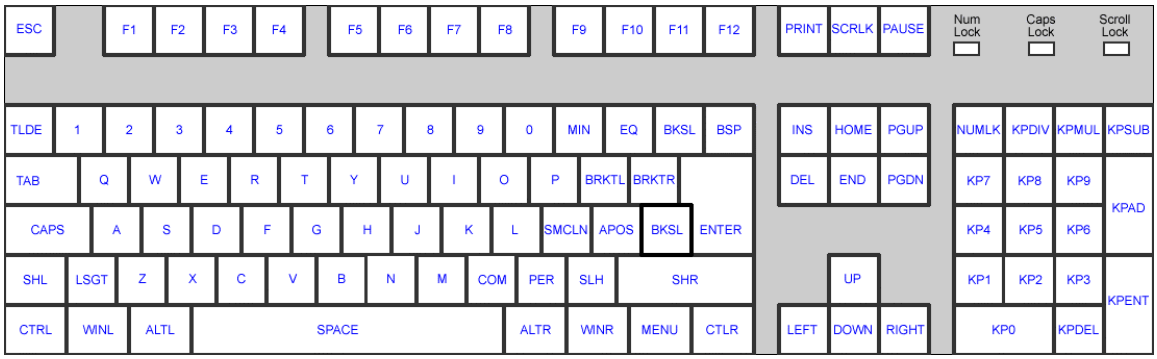
switches that provide hotkeys and/or OSD menu because it can simulate **any** keystroke sequence, not only the keys but also the time interval between them.
The sequence of keys that must be typed to select a given port is specific to the KVM switch attached to the KLE. However, usually the first two or three keys are fixed and they are followed by a variable sequence that corresponds to the KVM port. For example *Scrolllock–Scrolllock–1* to select port 1, *Scrolllock–Scrolllock–2* to select port two, and so on (If you need to open an OSD menu, this sequence can be more complex, however KLE can generate anything).
The first fixed part of the command is called here *Escape Hot Key Sequence*, and the variable part is called *Port Selection Sequence*.
Enter into the *Escape Hot Key Sequence* the fixed part of the KVM switch commands. If you have a doubt about the corresponding name for the keys, please refer to the keyboard drawing for reference. You can select up to 4 keys.

Delay Between Keys: Specify here the delay time in milliseconds (from 10 to 1000 milliseconds) that KLE must wait between keys. This delay is KVM-switch-dependant. Some KVM switches are fast and some are sluggish. To work out the optimal delay time, make a few port switching trials with different delay times.
Note: It is also possible to insert a precise delay between two specific keys if you need to increase the common delay value selected above. To do so, just type d (xxx), xxx being the value in milliseconds up to 1000. For example, d (50) makes a 50 millisecond extra delay.

KVM Key Sequence for Port Selection: Here you can edit the *Port Selection Sequence*s command strings with the following rules:.
1. Use one separate line for each port, and start from port #1.
2. Separate keycodes and delays with at least one space. Example: 0 1 0 2 d(300) ESC
3. Refer to the *keyboard diagram* to find out the right keycodes. The keycode for a specific key might not exactly correspond to what you can see on your local keyboard. Also reference the **CAUTION** warning on the bottom right of this page.
To select a port, KLE generates first the *Escape Hot Key Sequence* selected above, followed by the *Port Selection Sequence* into the line corresponding to the port number. This will make up a complete hotkey command for port selection.
For example: let us say that the *Escape Hot Key Sequence* is *Scrolllock – Scrolllock* and that in the *Port Selection Sequence*s area you have
1
2
3
…
7
8
These mean:
send out *Scrolllock – Scrolllock – 1* to select port #1
send out *Scrolllock – Scrolllock – 2* to select port #2
……
send out *Scrolllock – Scrolllock – 8* to select port #8

However, some other command strings you will see in the editable area might seem as complex as *0 1 0 1 d(1000) ESC*. For example: in the editable area suppose now you have:
0 1 0 1 d(1000) ESC
In other words, to select port #1: send out *ScrollLock–ScrollLock–0-1-0-1, then add a 1000-millisecond delay and then send out an Escape key*
0 1 0 2 d(1000) ESC
In other words, to select port #2: send out *ScrollLock–ScrollLock–0-1-0-2, then add a 1000-millisecond delay and then send out an Escape key*
…….
0 1 0 8 d(1000) ESC
In other words, to select port #8: send out *ScrollLock–ScrollLock–0-1-0-8, then add a 1000-millisecond delay and then send out an Escape key*

NB. The hotkey sequence *"0 1 0 1 ESC"* means switching to bank 01 port 01 and then revoke the OSD menu by an ESC key.



Store the (new) KVM Model Settings: If you want to suppress the target KVM Switch definition, you can then click the *Suppress* button to eliminate it from the existing database.

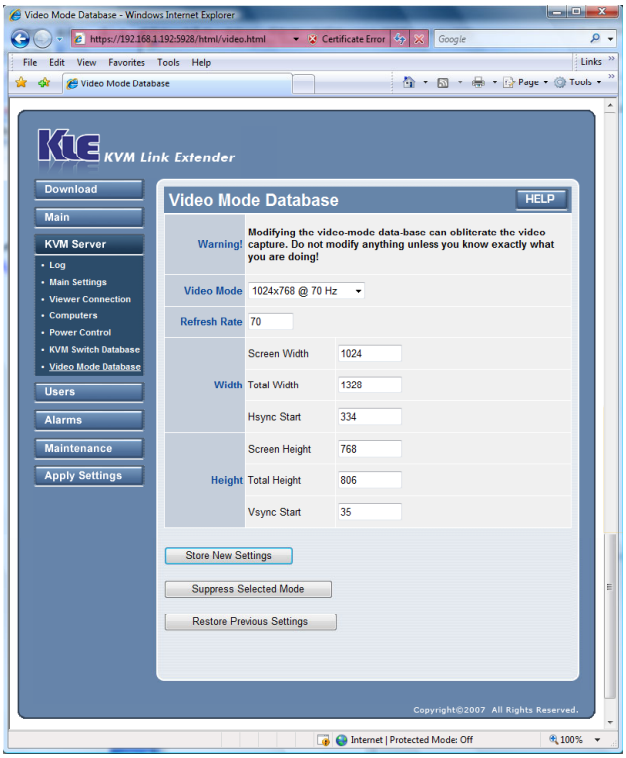
Suppress this KVM Model: After you have completed your settings of the port switching sequence of your KVM switch, you must hit *Store* to store the settings to the KVM database.

4.14 KVM Server/Video Mode Database –Modifying the Video Display Database

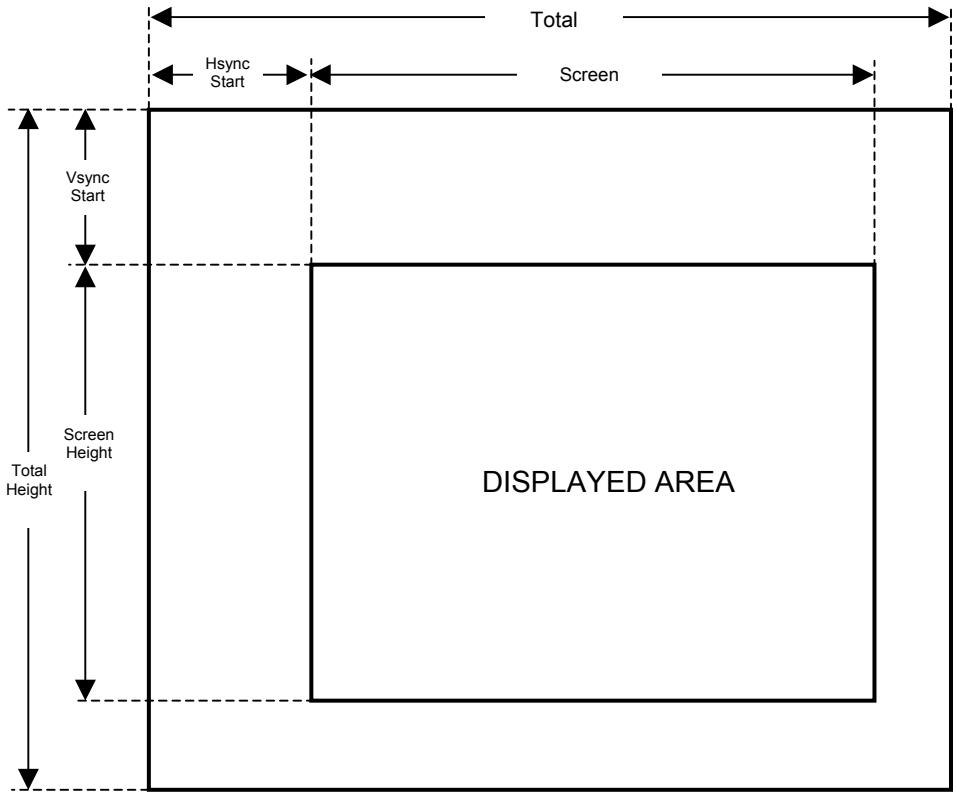
The Video Mode Database page allows you to modify, create and suppress the VGA modes supported by the device.
Important Note: Carelessly modifying a video mode on this video database might obliterate the video capture, thus DO NOT MODIFY anything unless you know exactly what you are doing.

After you have made all modifications, click *Store Settings* to save your settings and then hit Apply *Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



Use the drop down box to select a video mode from the video mode database. Each video mode is indicated by the pixel dimension (length by width) at a certain refresh frequency:
Width_in_pixels x Height_in_pixels @ Refresh_Rate_in_Hz
For example, 1024 x 768@60Hz is a video mode and 1024 X 768@72 Hz is another video mode. Together with the refresh rate and the pixel dimensions, a video mode can be adjusted with those parameters such as **screen width, total width, Hsync start**, as well as **screen height, total height, and Vsync start**.
The following diagram explains the geometric relations between the VGA parameters.



Refresh Rate: Here you can modify the refresh rate of the target VGA mode.

Width: Here you can modify the various width parameters of the target VGA mode:

- **Screen Width:** specify the width of the visible part of the screen.
- **Total Width:** specify the total width of the screen (active + hidden)
- **Hsync Start:** specify where the VGA horizontal synchronization should start with reference to the beginning of the line.

Height: Here you can modify the various height parameters of the target VGA mode:

- **Screen Height:** specify the height of the visible part of the screen.
- **Total Height:** specify the total height of the screen (active + hidden).
- **Vsync Start:** specify where the vertical synchronization should start with reference to the top of the page.

Store New Settings: Click this button to save your modification/addition to the video mode database.

Suppress Selected Mode: Click this button to remove the selected video mode from the video mode database. Normally, one does not have to suppress a video mode from the existing database for no particular purpose.

Restore Previous Settings: Click to undo the previous addition or elimination of a video mode. **Note** that you can only undo **one** move.

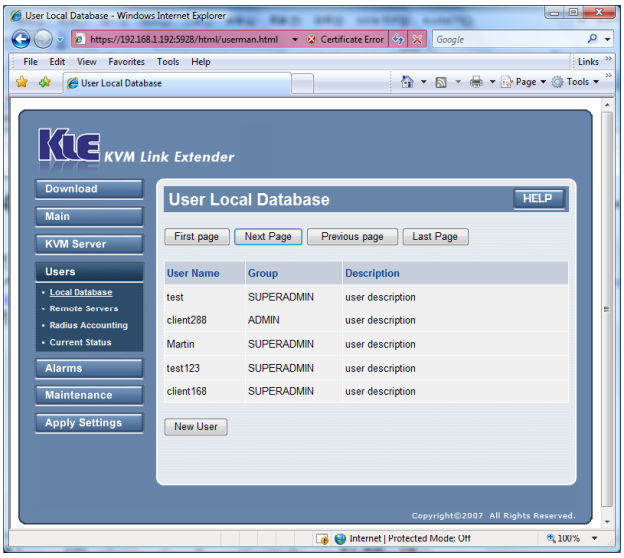
4.15 Users/Local Database - Managing the User Accounts

The User Local Database page is for the purpose of user account management for KLE. You can see the listing of the existing user entries, together with the user group the specific user belongs to and the description for the user.

You can use the buttons on the top row – *First Page/ Next Page/ Previous Page/Last Page* to navigate through the first/next/previous/last page of the user database listing.

To modify, add or delete an entry, click the target user name on the listing and a User Edit screen will appear for you to make further modifications or to create a new user entry.

After you have made necessary modifications, remember to hit the *Store User* button to save it into the user account database.



KLE offers three categories of user groups for selection: **SUPERADMIN, ADMIN and USER**.
Each of these user groups is with different rights into the web management Interface and into the viewers:

User Group	*Management*	*Viewer*
SUPERADMIN	Full access	All functions
ADMIN	Partial access (see table below)	All functions
USER	No access except the Download page	No power on/off feature

Note: Only SUPERADMIN users can manage user accounts.

Refer to the table below for detailed list of web management rights:

Management Page	*SUPERADMIN*	*ADMIN*	*USER*
Download/Viewer	x	x	x
Main/Date & Time	x	x	-
Main/Security	x	-	-
Main/LAN TCP-IP	x	-	-
Main/WAN PPP	x	-	-
KVM Server/Log	x	x	-
KVM Server/Main Settings	x	x	-
KVM Server/Viewer Connection	x	x	-
KVM Server/Computers	x	x	-
KVM Server/Power Control	x	x	-
KVM Server/KVM switch database	x	x	-
KVM Server/Video Mode database	x	x	-
Users/local database	x	-	-
Users/Remote [Authent] Servers	x	-	-
Users/Radius Accounting	x	-	-
Users/Current Status	x	-	-
Alarms/Emails	x	x	-
Alarms/SNMP	x	x	-
Alarms/Selection	x	x	-
Maintenance/Software Version	x	-	-
Maintenance/Software Upgrade	x	-	-
Maintenance/Config. Save/Restore	x	-	-
Maintenance/Reboot	x	-	-
Apply Settings/Restart Servers	x	x	-

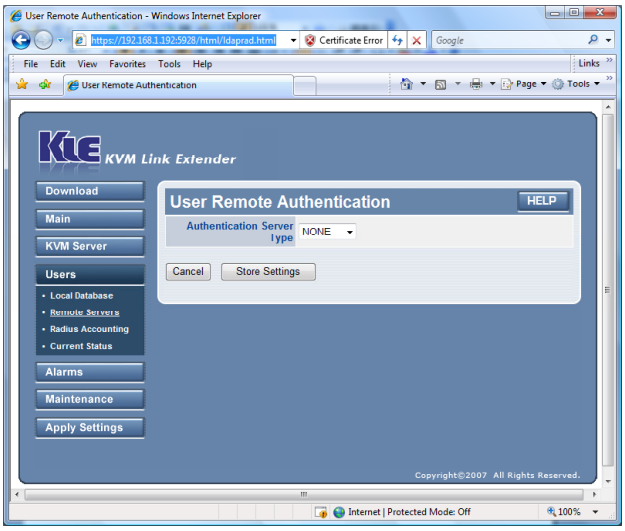
4.16 Users/Remote Servers – Tuning in with the Remote Authentication Servers

The User Remote Authentication allows you to authenticate the users that try to connect to KLE from centralized servers running a Radius service or hosting a directory that can be accessed through the LDAP protocol (Active Directory for example). This feature permits to integrate KLE into your global enterprise user management.

By default, the Remote Authentication is configured as *None*, i.e., all remote authentications are disabled. In this case, the authentication is all done locally by using the database on KLE only.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!

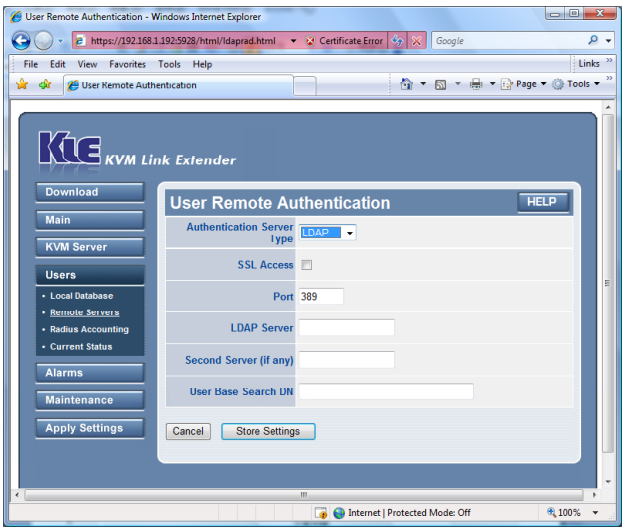


Authentication Server Type: Here you can select whether you want to disable, or enable the remote server authentication by LDAP or RADIUS server. Before you go forth with subsequent settings on this page, you should check with your network administrator for the availability of either a LDAP server or a RADIUS server.

- To disable the remote authentication support: Select *None* for the Authentication Server Type.
- To enable LDAP authentication support: Select *LDAP* for the Authentication Server Type.
- To enable RADIUS authentication support: Select *RADIUS* for the Authentication Server Type.

4.16.1 Directory Server

Using LDAP SSL Access: Check this option if you want to enable SSL access of the LDAP authentication. However, to use this option, you should make sure your LDAP server support SSL, and also you have to install a distinct set of certificates – ldapcert.crt and ldapkey.pem – onto KLE by uploading them through the *Security page*. Normally these certificates are generated by the directory server itself.



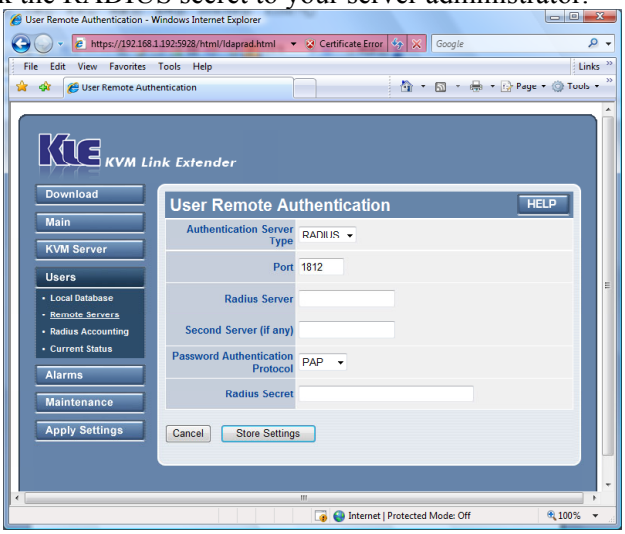
Port: Enter here the port number used in LDAP authentication. By default, it is set to port **389**.

LDAP Server: Enter here the IP address of the directory server.
Second Server (if any): If there is a second LDAP server available for authentication, enter its IP address here.

User Base Search DN: Here you should enter the User Base Search DN, which is typical to the LDAP server you use for authentication. By default, the User Base Search DN is:
cn=users, dc=abc, dc=KLE, dc=com
However, you should enter your own appropriate one. If you don't know, you should contact your LDAP server administrator.

4.16.2 RADIUS Server

Port: Enter here the port number used in RADIUS authentication. By default, it is set to port **1812**.
RADIUS Server: Enter here the IP address of the RADIUS server.
RADIUS server authentication: If there is a second RADIUS server for authentication, enter its IP address here.
Password Authentication Protocol: Select the password authentication protocol to be either CHAP or PAP.
RADIUS secret: Specify here the RADIUS secret (or Shared Secret), between the KLE and the RADIUS server. Note that the RADIUS secret is a text string that is used as a password between the RADIUS client and the RADIUS server. Ask the RADIUS secret to your server administrator.



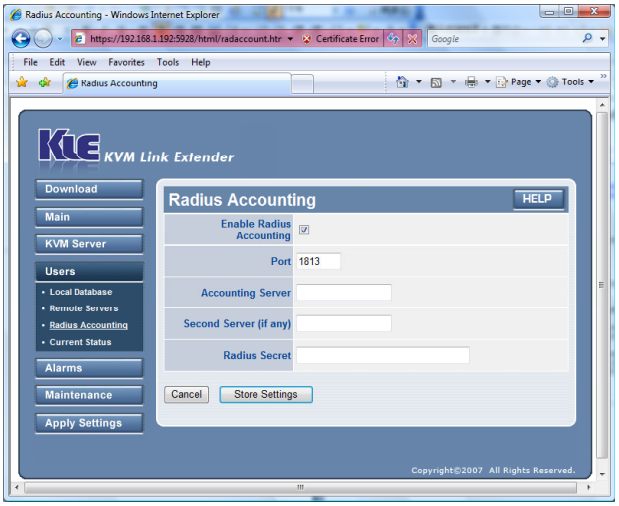
4.17 Users/Radius Accounting

Normally, RADIUS accounting is disabled by default. However, if you have RADIUS accounting enabled on a RADIUS server or LDAP server, you can check the option of RADIUS Accounting and subsequently configure its relevant settings to take advantage of this feature.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!

Enable RADIUS Accounting: Check this option, if you want to enable RADIUS accounting support on Prima IP.



Accounting Server: Here you should enter the IP address of the server that offers RADIUS accounting service.

Port: Here you should specify the port that is used for Radius accounting. By default, it is set to 1813.

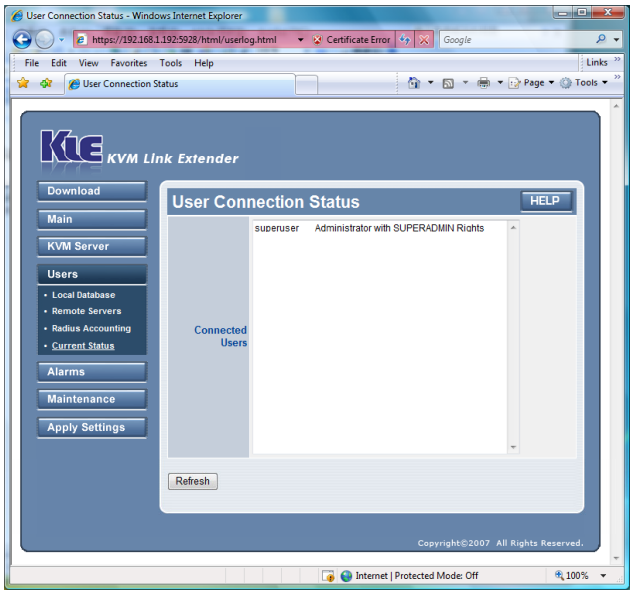
Secondary Accounting Server (if any): Here you should enter the IP address of the secondary server, if you've got any backup RADIUS accounting server that offers RADIUS accounting service.

RADIUS secret: Here you should specify the RADIUS secret, or Shared Secret, between the RADIUS client (i.e. Prima IP) and the RADIUS server. Note that the RADIUS secret, or the Shared Secret, is a shared text string that is used as a password between the RADIUS client and RADIUS server.

4.18 Users/Current Status – Showing the Currently Connected Users

This page will show the remote users that are connected at the time you access this status page. However, this status page will not refresh itself. In order to know whether there is any change to the connection status, you should refresh this page by clicking the *Refresh* button for current information on connected users.

> **Important Note:** Only when you have selected your password policy to be *User Password* policy, will the currently connected users be registered and shown on this page. If you are using other password policies such as *No Password* or *Global Password*, you will not have any connected users shown on this page, since when adopting these policies you imply that the distinction of user identities is not necessary. For more information on password policies, please refer to the *Security* page.

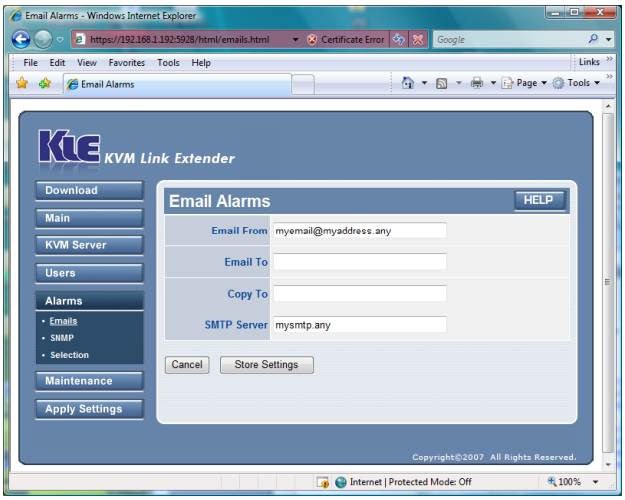


4.19 Alarms/Emails – Sending Email Notifications for Critical Server Events

This page allows you to set up the email notification for alarm events.

After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.

No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



Email from: Sender email address used by the KLE for alarm emails, for example:

myemail@myaddress.any.

It must be accepted by the SMTP server. This email address can help identify which KLE is the sender.

Email to: e-mail address of KLE alarm email addressee.

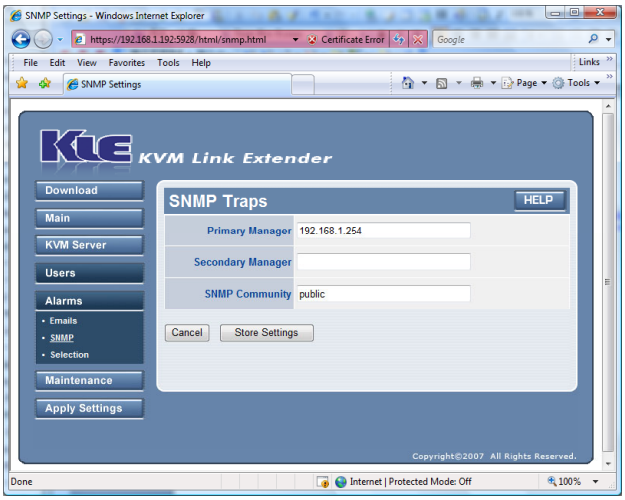
Note: You can use commas for multiple recipients: support@myaddress.net, emma@international.com, joe@netview.co.jp

Copy to: e-mail address of addressees who should get a “carbon copy” of alarm emails.

SMTP Server: Enter the name or IP address of the SMTP server (mail server) that will route the KLE email alarms to recipients

4.20 Alarms/SNMP – Sending SNMP Messages for Critical Server Events

Here you can set up the SNMP traps sent by KLE, provided you selected the SNMP traps somewhere into the *Alarm* page.
After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.
No change you have made on this page will apply until you hit *Apply Settings/Restart Servers*!



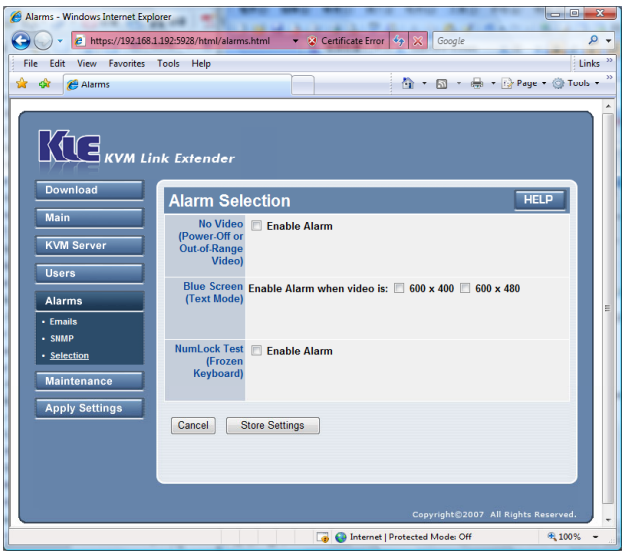
Primary Manager: Specify here the IP address of the Primary SNMP manager device on your network.

Secondary Manager: Specify here the IP address of the Secondary SNMP manager device on your network (if any).
SNMP Community: Specify here the name of the SNMP Community to which your SNMP Management host and SNMP agent should belong.
Note: the SNMP manager and agents must belong to an SNMP community identified by its name, which is a collection of hosts grouped together for administrative purposes.

4.21 Alarms/Selections – Select the Alarm-triggering Events

KLE is capable of sending immediate alerts, as emails or SNMP traps, and/or performing automatically a power cycling when there is blue screen, no video, or NumLock test failure from a remote computer. This feature should be used in conjunction with the *autoscanning* function, so that KLE will help carry on a constant surveillance on the health conditions of your connected servers.

> **Note:** This *Alarm Selection* page is where you can select which action KLE must do when it detects an event. This page is NOT the place where you can specify how the action is to be implemented. To do so, refer to SNMP Traps, Email Alarms and Computers.
> After you have made all modifications, click *Store Settings* to save your settings and then hit *Apply Settings/Restart Servers* to validate these new settings.
> No change you have made on this page will apply until you hit *Apply Settings/Restart* Servers!

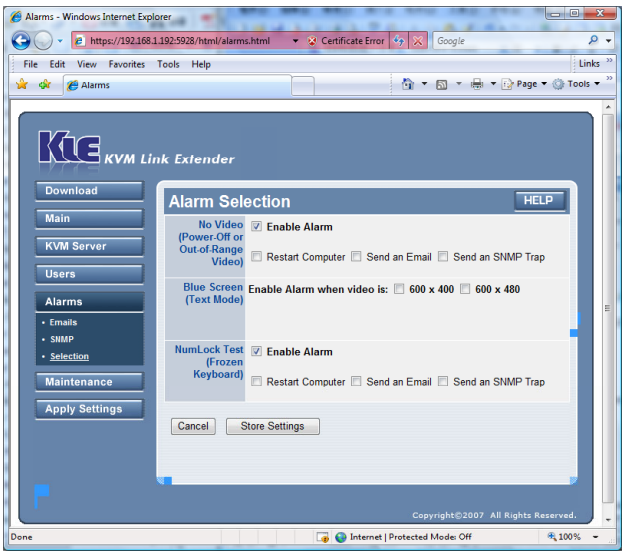


KLE can respond to three types of alarm-triggering events:

- No Video
- Blue Screen
- NumLock test failure.

Each one of these events can be configured to trigger any one of these three types of actions:

- Send an email,
- Send an SNMP trap message,
- Restart the computer (Power cycling).



No Video Alarm (Blank Screen): No Video could be a result from power failure or an unsupported video mode, i.e., an out-of-range video mode or most often a video mode not yet set up into the video database. If you want KLE to respond immediately to this sort of events, just check the Enable Alarm option, then specify what type(s) of action you would like to do: either Restart Computer, Send an Email, or Send an SNMP trap.

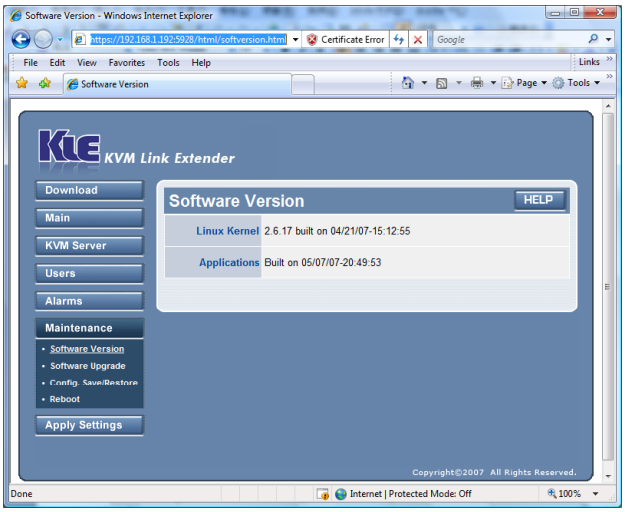
Blue Screen Alarm (Text mode): Blue screen is a result of Windows Operating System fatal error. A blue screen can be detected by its low-resolution video mode.
If you want KLE to respond immediately to this event, just check the Enable Alarm option. Next specify what type(s) of screen resolution you will regard as Blue Screen: 600 x 400 or 600 x 480, and subsequently select either Restart Computer, Send an Email, or Send an SNMP trap as action to do.

NumLock Test Alarm (Frozen Keyboard): The NumLock test is to send a NumLock signal to the computer, and the computer normally should return a response immediately so that the NumLock LED indicator on the keyboard will be lit to indicate the success of the test. The failure of a NumLock test indicates at least a keyboard failure to respond to this NumLock signal, or it might be due to bigger problem such as system failure, or simply a powered-off state.
If you want KLE to respond to this alarm-triggering event, just check the Enable Alarm option. Next specify what type(s) of action you would like to do: Restart Computer, Send an Email, or Send an SNMP trap.

4.22 Maintenance/Software Version – Flash Image Information

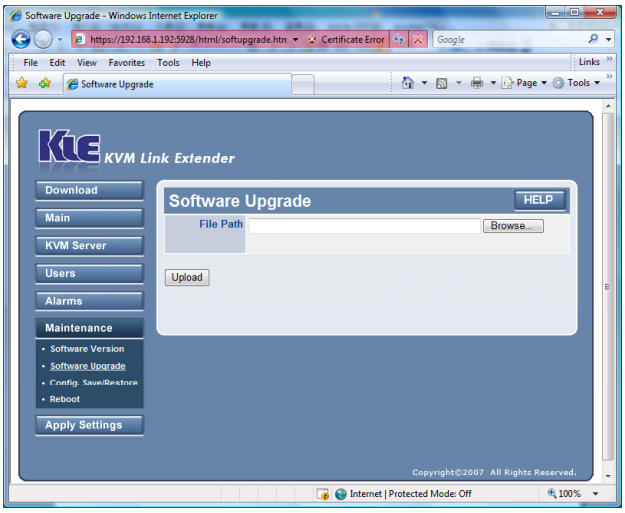
The Software version page shows the current software version information. For example, here you can check the Linux kernel version, and the time it is built, together with the software-application build and its time stamp.

Linux Kernel 2.6.17 built on 04/21/07-15:12:55
Applications Built on 05/07/07-20:49:53



4.23 Maintenance/Software Upgrade –Upgrading the Software via Web

The *Software Upgrade* page is where you can browse to the path location of software upgrade file, and upload it to KLE across the LAN or the Internet.



Note: the KLE upgrade file must have a name starting with "tkip101" followed by the date, such as tkip101-yy-mm-dd (for example tkip101-07-03-29).

Note: The upgrade file is of an accumulative nature, which means that normally you only have to apply the single latest upgrade patch to keep your KLE most up-to-date.

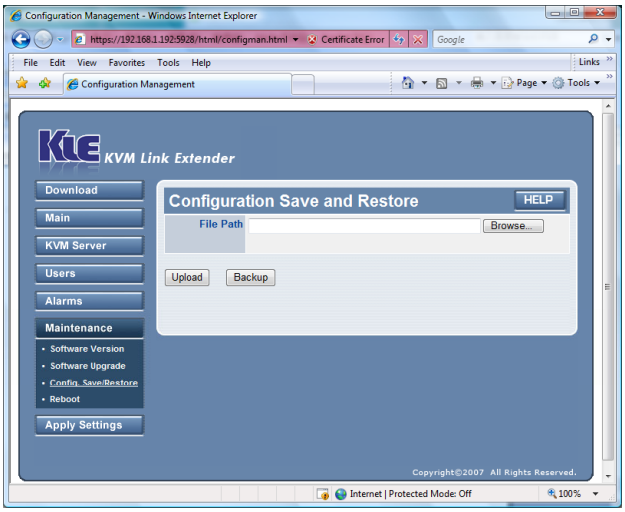
When you receive the upgrade file, you must first copy it to a local computer. Then use the KLE's Web management interface to perform the update across your LAN or across the Internet.

Performing a software upgrade

Just hit the *Browse* button to browse to the location of the update file and then click *Upload*. A running progress indicator bar will be running to indicate the on-going upload process. Depending on the upgrade file size and the bandwidth availability across the network, file upload time could vary from 1 minute to 20 minutes. When the upload process is complete, KLE will reboot by itself. After the reboot is completed, it should be working right away.

4.24 Maintenance/Configuration Save and Restore

This page allows you to save your current KLE settings to a single .tgz file for more portability and usability. It is wise to backup your configuration after any change. It can be used also to set up several KLE with same or similar configuration.



To backup the configuration file

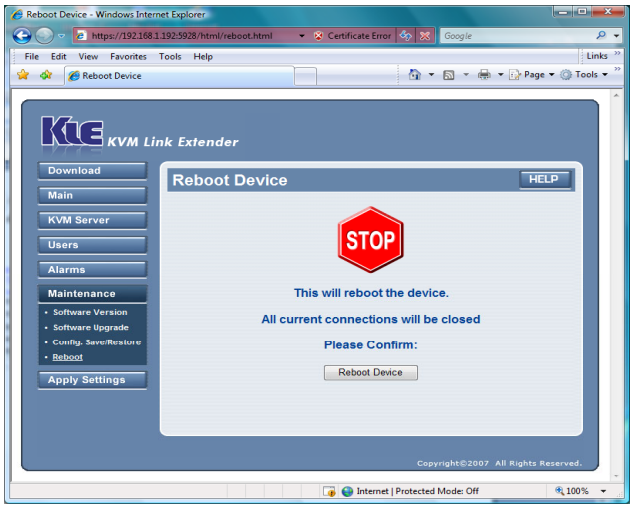
Click the *Backup* button, choose the location for saving your configuration file (*.tgz), and then click *Save*. The configuration file name format is: kconfig-yyyymmdd.tgz, with a timestamp in it.

To upload the configuration file

Hit the *Browse* button to browse to the location of the update file (kconfig-yyyymmdd.tgz) and then click *Upload* . You will be prompted for a reboot when the upload process is complete. Reboot to validate the new configuration.

4.25 Maintenance/Reboot – Configuration Backup and upload

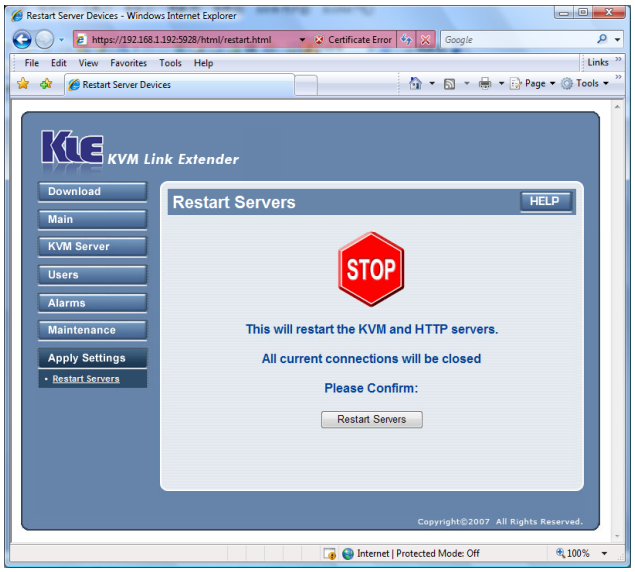
In case your KLE has crashed and beyond restoration, simply by hitting the *Apply Settings/Restart* Servers button, you can always have the last resort to completely reboot the KLE from ground level up by hitting the *Reboot Device* button.



In most of the cases, you do not need to use this *Reboot* button to restart your KLE. Normally, you should use the *Apply Settings* button on the *Apply Settings* page for almost all the cases of restarting/rebooting KLE with new settings. However, if you find the *Apply Setting/Restart Servers* button could not bring the KLE to a restart that works properly with the viewer, you can then try to use the *Reboot* button here. However, as a rule of thumb, you should try the *Apply Settings/Restart Servers* button first, before you try the *Reboot* button here on this page.

4.26 Apply Settings/Restart Servers – Validate New Settings & Restart Video Servers

All the new settings you have made could only be committed to the KLE's database by clicking the **Store Settings/Store/Store User** button on each setting page. However, just clicking any of these buttons won't have these new settings immediately validated. You should hit the *Restart Servers* button so that new settings can be put into use at once.



Note: The *Restart Servers* button will disconnect all current viewer connections.

Note: In addition to the *Restart Servers* button, the KLE also provides an *Reboot* button (on Maintenance/Reboot page). This *Reboot* button is used only when the *Restart Servers* button could works no longer to bring the KLE to normal restart for a proper viewer connection. If you find the *Restart Servers* button no longer works to bring the KLE to an effective restart, you can click the *Reboot* button on the Maintenance/Reboot Page. Only bear in mind that the reboot brought about by hitting the *Reboot* button is a total reboot and takes longer time to boot up completely, while *Restart Servers* is much quicker (just few seconds) since it restarts only the server programs on the KLE.